

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/000532

International filing date: 18 January 2005 (18.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-016894  
Filing date: 26 January 2004 (26.01.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

19.01.2005

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年 1月26日  
Date of Application:

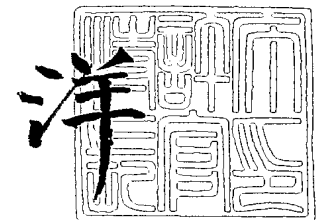
出願番号 特願2004-016894  
Application Number:  
[ST. 10/C]: [JP2004-016894]

出願人 日本電気株式会社  
Applicant(s):

2004年 8月30日

特許庁長官  
Commissioner,  
Japan Patent Office

小川



出証番号 出証特2004-3077571

【書類名】 特許願  
【整理番号】 35001254  
【提出日】 平成16年 1月26日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 17/60  
【発明者】  
    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内  
    【氏名】 森 健吾  
【発明者】  
    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内  
    【氏名】 佐古 和恵  
【特許出願人】  
    【識別番号】 000004237  
    【氏名又は名称】 日本電気株式会社  
【代理人】  
    【識別番号】 100123788  
    【弁理士】  
    【氏名又は名称】 宮崎 昭夫  
    【電話番号】 03-3585-1882  
【選任した代理人】  
    【識別番号】 100088328  
    【弁理士】  
    【氏名又は名称】 金田 暢之  
【選任した代理人】  
    【識別番号】 100106297  
    【弁理士】  
    【氏名又は名称】 伊藤 克博  
【選任した代理人】  
    【識別番号】 100106138  
    【弁理士】  
    【氏名又は名称】 石橋 政幸  
【手数料の表示】  
    【予納台帳番号】 201087  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 0304683

**【書類名】 特許請求の範囲****【請求項 1】**

投票者が投票を行うための投票機器と、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

暗号投票データを再度暗号化する再暗号化手段を備え、前記投票機器から受信した暗号投票データを再度暗号化して当該投票機器に返信する暗号サーバと、

候補者名とその候補者名を暗号化した暗号投票データとの組のリストを前記投票機器に送信し、その後、認証情報をもとに前記投票者が有権者であることと未投票であることを確認したのちに前記投票機器からの暗号投票データを受付け、受信した有効な暗号投票データのリストを投票期間終了後に前記匿名復号システムに送信する投票サーバと、

を有し、

前記投票機器は、前記投票サーバから前記リストを受信した後に、前記投票者が選択した候補者名に対応する暗号投票データを前記暗号サーバに送信し、前記暗号サーバで再度暗号化された暗号投票データを受信して前記投票サーバに送信するとともに、前記投票者の認証情報を前記投票サーバに送信する、匿名電子投票システム。

**【請求項 2】**

投票者が投票を行うための投票機器と、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

暗号投票データを再度暗号化する再暗号化手段をそれぞれ備え、前記投票機器から受信した暗号投票データを再度暗号化して当該投票機器に返信する複数の暗号サーバと、

候補者名とその候補者名を暗号化した暗号投票データとの組のリストを前記投票機器に送信し、その後、認証情報をもとに前記投票者が有権者であることと未投票であることを確認したのちに前記投票機器からの暗号投票データを受付け、受信した有効な暗号投票データのリストを投票期間終了後に前記匿名復号システムに送信する投票サーバと、

を有し、

前記投票機器は、前記投票サーバから前記リストを受信した後に、前記投票者が選択した候補者名に対応する暗号投票データを最初の暗号サーバに送信して該最初の暗号サーバから再度暗号化された暗号投票データを受信し、受信した再度暗号化された暗号投票データを次の暗号サーバに送信して該次の暗号サーバから再度暗号化された暗号投票データを受信する処理を最後の暗号サーバから再度暗号化された暗号投票データを受信するまで繰り返し、前記最後の暗号サーバから送信されてきた再度暗号化された暗号投票データを前記投票サーバに送信するとともに、前記投票者の認証情報を前記投票サーバに送信する、匿名電子投票システム。

**【請求項 3】**

認証サーバと、

投票者が投票を行うための投票機器であって、前記認証サーバに対してデジタル署名によらない手順で前記投票者の認証を行わせるとともに、暗号投票データを前記認証サーバに送信する投票機器と、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを匿名復号システムに送信する投票サーバと、

を有し、

前記認証サーバは、前記投票機器から受信した暗号投票データに投票者名を付加して該認証サーバのデジタル署名を付与して投票サーバに送信する、匿名電子投票システム。

**【請求項 4】**

認証サーバと、

投票者が投票を行うための投票機器であって、特定の組織内部でのみ検証可能な前記投票者のデジタル署名を付与して暗号投票データを前記認証サーバに送信する投票機器と、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを匿名復号システムに送信する投票サーバと、

を有し、

前記認証サーバは、前記投票機器から受信したデジタル署名を検証してから、暗号投票データに投票者名を付加して該認証サーバのデジタル署名を付与して前記投票サーバに送信する、匿名電子投票システム。

#### 【請求項 5】

認証サーバと、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを匿名復号システムに送信する投票サーバと、

を有し、

前記認証サーバは、投票者をデジタル署名によらない手段で認証するとともに投票機器から該投票者の暗号投票データを受け取り、受け取った暗号投票データに投票者名を付加して認証サーバのデジタル署名を付与して投票サーバに送信し、また、投票機器から特定の組織内部でのみ検証可能なデジタル署名の付与された暗号投票データを受信したときは、デジタル署名を検証したのちに暗号投票データに投票者名を付加して認証サーバのデジタル署名を付与して投票サーバに送信する、匿名電子投票システム。

#### 【請求項 6】

投票者が投票を行うための投票機器と、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

公開情報から第 1 の変換データを生成する第 1 の変換手段を備え、前記第 1 の変換データを前記投票機器に送信する投票サーバと、

公開情報から第 2 の変換データを生成する第 2 の変換手段をそれぞれ備えて前記第 2 の変換データを前記投票機器に送信する 1 または複数の暗号サーバと、

を有し、

前記投票機器は、前記投票サーバから受信した第 1 の変換データと前記各暗号サーバからそれぞれ受信した第 2 の変換データを用いて、投票者が記述した投票内容を暗号化して暗号投票データを作成して前記投票サーバに送信し、かつ、前記投票者の認証情報を前記投票サーバに送信し、

前記投票サーバは、前記認証情報をもとに前記投票者が有権者であることと未投票であることを確認したのちに暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、匿名電子投票システム。

#### 【請求項 7】

投票者が投票を行うための投票機器と、

受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、

公開情報から第 2 の変換データを生成する第 2 の変換手段をそれぞれ備えて前記第 2 の変換データを前記投票機器に送信する複数の暗号サーバと、

を有し、

前記投票機器は、前記各暗号サーバからそれぞれ受信した第2の変換データを用いて、投票者が記述した投票内容を暗号化して暗号投票データを作成して前記投票サーバに送信し、かつ、前記投票者の認証情報を前記投票サーバに送信し、

前記投票サーバは、前記認証情報をもとに前記投票者が有権者であることと未投票であることを確認したのちに暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、匿名電子投票システム。

【請求項8】

前記投票機器は、暗号投票データとともに暗号化証明データを作成し、暗号投票データとともに前記暗号化証明データを前記投票サーバに送信し、

前記投票サーバは、前記投票者が有権者であることと未投票であることを確認後、前記暗号化証明データを検証して合格であれば前記投票機器からの暗号投票データを受付ける、請求項6または7に記載の匿名電子投票システム。

【請求項9】

前記投票サーバは、候補者名とその候補者名を暗号化した暗号投票データと候補者名を正しく暗号化したことの証明データとの組のリストを前記投票機器に送信し、

前記暗号サーバは、前記投票機器から受信した暗号投票データを再度暗号化するとともにその暗号投票データを正しく再度暗号化したことを示す証明データを作成して前記投票機器に返信する、請求項1または2に記載の匿名電子投票システム。

【請求項10】

さらに認証サーバを備え、

前記投票機器は、暗号投票データを前記投票サーバに送信する代わりに、前記認証サーバに対してデジタル署名によらない手段で前記投票者の認証を行なわせてから暗号投票データを前記認証サーバに送信し、

前記認証サーバは、受信した暗号投票データに投票者名を付加して認証サーバのデジタル署名を付与して投票サーバに送信し、

前記投票サーバは、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、請求項1、2、6、7、8及び9のいずれか1項に記載の匿名電子投票システム。

【請求項11】

さらに認証サーバを含み、

前記投票機器は、暗号投票データを前記投票サーバに送信する代わりに、特定の組織内部でのみ検証可能な前記投票者のデジタル署名を付与して暗号投票データを前記認証サーバに送信し、

前記認証サーバは、前記投票機器から受信したデジタル署名を検証してから、暗号投票データに投票者名を付加して該認証サーバのデジタル署名を付与して前記投票サーバに送信し、

前記投票サーバは、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、請求項1、2、6、7、8及び9のいずれか1項に記載の匿名電子投票システム。

【請求項12】

さらに認証サーバを含み、

前記認証サーバは、投票者をデジタル署名によらない手段で認証するとともに前記投票機器から暗号投票データを受け取り、受け取った暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して前記投票サーバに送信し、また、前記投票機器から特定の組織内部でのみ検証可能なデジタル署名の付与された暗号投票データを受信する

と、前記デジタル署名を検証したのちに暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して前記投票サーバに送信し、

前記投票サーバは、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、請求項1、2、6、7、8及び9のいずれか1項に記載の匿名電子投票システム。

【請求項13】

投票サーバと投票者が投票を行うための投票機器と暗号サーバと匿名復号システムとを用いる匿名電子投票方法であって、

前記投票サーバが、候補者名を暗号化して候補者名とその候補者名を暗号化した暗号投票データとの組のリストを投票機器に送信する段階と、

前記投票機器が、前記投票者が選択した候補者名と組となった暗号投票データを前記暗号サーバに送信する段階と、

前記暗号サーバが、受信した暗号投票データを再度暗号化して前記投票機器に返信する段階と、

前記投票機器が、前記暗号サーバから受信した暗号投票データを前記投票サーバに送信するとともに、前記投票者の認証情報を前記投票サーバに送信する段階と、

前記投票サーバが、前記認証情報をもとに投票者が有権者であることと未投票であることを確認したのちに前記投票機器からの暗号投票データを受付ける段階と、

前記投票サーバが、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する段階と、

前記匿名復号システムが、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

を有する匿名電子投票方法。

【請求項14】

投票サーバと、投票者が投票を行うための投票機器と、暗号投票データを再度暗号化する再暗号化手段をそれぞれ備える複数の暗号サーバと、匿名復号システムと、を用いる匿名電子投票方法であって、

前記投票サーバが、候補者名とその候補者名を暗号化した暗号投票データとの組のリストを前記投票機器に送信する段階と、

前記投票機器が、前記投票者が選択した候補者名に対応する暗号投票データを最初の暗号サーバに送信して該最初の暗号サーバから再度暗号化された暗号投票データを受信し、受信した再度暗号化された暗号投票データを次の暗号サーバに送信して該次の暗号サーバから再度暗号化された暗号投票データを受信する処理を最後の暗号サーバから再度暗号化された暗号投票データを受信するまで繰り返し、前記最後の暗号サーバから送信されてきた再度暗号化された暗号投票データを前記投票サーバに送信するとともに、前記投票者の認証情報を前記投票サーバに送信する段階と、

前記投票サーバが、認証情報をもとに投票者が有権者であることと未投票であることを確認したのちに前記投票機器からの暗号投票データを受付ける段階と、

前記投票サーバが、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する段階と、

匿名復号システムが、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

を有する、匿名電子投票方法。

【請求項15】

投票サーバと投票機器と認証サーバと匿名復号システムとを用いる匿名電子投票方法であって、

前記投票機器が、前記認証サーバに対してデジタル署名によらない手段で投票者の認証を行なわせるとともに、暗号投票データを前記認証サーバに送信する段階と、

前記認証サーバが、受信した暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して前記投票サーバに送信する段階と、

前記投票サーバが、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付ける段階と、

前記投票サーバが、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する段階と、

前記匿名復号システムが、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

を有する匿名電子投票方法。

【請求項 16】

投票サーバと投票機器と認証サーバと匿名復号システムとを用いる匿名電子投票方法であって、

前記投票機器が、暗号投票データに対して特定の組織内部でのみ検証可能な投票者のデジタル署名を付与して前記認証サーバに送信する段階と、

前記認証サーバが、受信したデジタル署名を検証してから、暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して前記投票サーバに送信する段階と、

前記投票サーバが、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付ける段階と、

前記投票サーバが、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する段階と、

前記匿名復号システムが、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

を有する匿名電子投票方法。

【請求項 17】

投票サーバと投票機器と認証サーバと匿名復号システムとを用いる匿名電子投票方法であって、

前記認証サーバが、デジタル署名によらない手法で投票者を認証するとともに前記投票機器から暗号投票データを受け取り、その暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して投票サーバに送信し、また、前記投票機器から特定の組織内部でのみ検証可能なデジタル署名の付与された暗号投票データを受信すると、当該デジタル署名を検証したのちに暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して前記投票サーバに送信する段階と、

前記投票サーバが、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付ける段階と、

前記投票サーバが、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する段階と、

前記匿名復号システムが、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

を有する匿名電子投票方法。

【請求項 18】

公開情報から第1の変換データを生成する第1の変換情報を備える投票サーバと、投票機器と、公開情報から第2の変換データを生成する第2の変換手段をそれぞれ備える1または複数の暗号サーバと、匿名復号システムと、を用いる匿名電子投票方法であって、

前記投票サーバが前記第1の変換データを前記投票機器に送信する段階と、

前記各暗号サーバがそれぞれ前記第2の変換データを前記投票機器に送信する段階と、

前記投票機器が、前記投票サーバから受信した第1の変換データと前記各暗号サーバからそれぞれ受信した第2の変換データを用いて、投票者が記述した投票内容を暗号化した

暗号投票データを作成して前記投票サーバに送信するとともに、前記投票者の認証情報を前記投票サーバに送信する段階と、

前記投票サーバが前記認証情報をもとに前記投票者が有権者であることと未投票であることを確認したのちに前記投票機器からの暗号投票データを受付ける段階と、

前記投票サーバが、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する段階と、

前記匿名復号システムが、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

を有する匿名電子投票方法。

【請求項 19】

前記投票機器は、暗号投票データとともに暗号化証明データを作成し、暗号投票データとともに前記暗号化証明データを前記投票サーバに送信し、

前記投票サーバは、前記投票者が有権者であることと未投票であることを確認後、前記暗号化証明データを検証して合格であれば前記投票機器からの暗号投票データを受付ける、請求項 18 に記載の匿名電子投票方法。

【請求項 20】

前記投票サーバは、候補者名とその候補者名を暗号化した暗号投票データと候補者名を正しく暗号化したことの証明データとの組のリストを前記投票機器に送信し、

前記暗号サーバは、前記投票機器から受信した暗号投票データを再度暗号化するとともに暗号投票データを正しく再度暗号化したことを示す証明データを作成して前記投票機器に返信する、請求項 13 または 14 に記載の匿名電子投票方法。

【請求項 21】

さらに認証サーバを使用し、

前記投票機器は、暗号投票データを前記投票サーバに送信する代わりに、前記認証サーバに対してデジタル署名によらない手段で前記投票者の認証を行なわせてから暗号投票データを前記認証サーバに送信し、

前記認証サーバは、受信した暗号投票データに投票者名を付加して認証サーバのデジタル署名を付与して投票サーバに送信し、

前記投票サーバは、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、請求項 13、14、18、19 及び 20 のいずれか 1 項に記載の匿名電子投票方法。

【請求項 22】

さらに認証サーバを使用し、

前記投票機器は、暗号投票データを前記投票サーバに送信する代わりに、特定の組織内部でのみ検証可能な前記投票者のデジタル署名を付与して暗号投票データを前記認証サーバに送信し、

前記認証サーバは、前記投票機器から受信したデジタル署名を検証してから、暗号投票データに投票者名を付加して該認証サーバのデジタル署名を付与して前記投票サーバに送信し、

前記投票サーバは、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、請求項 13、14、18、19 及び 20 のいずれか 1 項に記載の匿名電子投票方法。

【請求項 23】

さらに認証サーバを使用し、

前記認証サーバは、投票者をデジタル署名によらない手段で認証するとともに前記投票機器から暗号投票データを受け取り、受け取った暗号投票データに投票者名を付加して前

記認証サーバのデジタル署名を付与して前記投票サーバに送信し、また、前記投票機器から特定の組織内部でのみ検証可能なデジタル署名の付与された暗号投票データを受信すると、前記デジタル署名を検証したのちに暗号投票データに投票者名を付加して前記認証サーバのデジタル署名を付与して前記投票サーバに送信し、

前記投票サーバは、前記認証サーバのデジタル署名が正しいことを確認し、投票者名が有権者名簿に記載されていることと未投票であることを確認して前記認証サーバからの暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを前記匿名復号システムに送信する、請求項 13、14、18、19 及び 20 のいずれか 1 項に記載の匿名電子投票方法。

【請求項 24】

匿名電子投票システムにおいて用いられる投票サーバであって、平文の投票内容を暗号化する暗号化手段を有する投票サーバ。

【請求項 25】

匿名電子投票システムにおいて用いられる暗号サーバであって、暗号投票データを再度暗号化する再暗号化手段を備える暗号サーバ。

【請求項 26】

匿名電子投票システムにおいて用いられる投票サーバであって、公開情報に基づいて変換データを生成する変換手段を備える投票サーバ。

【請求項 27】

匿名電子投票システムにおいて用いられる暗号サーバであって、公開情報に基づいて変換データを生成する変換手段を備える暗号サーバ。

【請求項 28】

匿名電子投票システムにおいて投票者が投票を行うために用いられる投票機器であって、平文の投票データと、第 1 のサーバから受信した第 1 の変換データと、前記第 1 のサーバとは異なる第 2 のサーバから受信した第 2 の変換データとに基づいて暗号投票データを作成する暗号化手段を有する、投票機器。

【請求項 29】

投票者の認証を行う認証サーバであって、デジタル署名によらずに前記投票者の ID の認証を行なう認証手段と、組織の内部向けの ID と全有権者に共通の ID との変換を行う ID 連携手段と、共通基盤における前記認証サーバのデジタル署名を作成する共通基盤署名生成と、を有する認証サーバ。

【請求項 30】

匿名電子投票システムにおいて投票者が投票を行うために用いられる投票機器であって、デジタル署名によらずに前記投票者の ID の認証を行なう認証手段を有する投票機器。

【請求項 31】

投票者の認証を行う認証サーバであって、特定の組織の内部向けに作成されたデジタル署名を検証する組織内署名検証手段と、組織の内部向けの ID と全有権者に共通の ID との変換を行う ID 連携手段と、共通基盤における認証サーバのデジタル署名を作成する共通基盤署名生成と、を有する認証サーバ。

【請求項 32】

匿名電子投票システムにおいて投票者が投票を行うために用いられる投票機器であって、特定の組織の内部向けのデジタル署名を生成する組織内署名生成手段を有する投票機器。

【請求項 33】

コンピュータに、  
候補者名とその候補者名を暗号化した暗号投票データとの組のリストを投票サーバから受信する処理と、  
投票者が選択した候補者名と組となった暗号投票データを暗号サーバに送信する処理と、

前記暗号サーバから受信した暗号投票データと前記投票者の認証情報とを前記投票サーバに送信する処理と、

バまたは認証サーバに送信する処理と、  
を実行させるプログラム。

【請求項 34】

コンピュータに、  
候補者名とその候補者名を暗号化した暗号投票データとの組のリストを投票サーバから受信する処理と、  
投票者が選択した候補者名に対応する暗号投票データを最初の暗号サーバに送信して該最初の暗号サーバから再度暗号化された暗号投票データを受信する処理と、  
受信した再度暗号化された暗号投票データを次の暗号サーバに送信して該次の暗号サーバから再度暗号化された暗号投票データを受信する処理を最後の暗号サーバから再度暗号化された暗号投票データを受信するまで繰り返す処理と、  
前記最後の暗号サーバから送信されてきた再度暗号化された暗号投票データを前記投票サーバに送信するとともに、前記投票者の認証情報を前記投票サーバに送信する処理と、  
前記暗号サーバから受信した暗号投票データと前記投票者の認証情報とを前記投票サーバまたは認証サーバに送信する処理と、  
を実行させるプログラム。

【請求項 35】

コンピュータに、  
投票サーバから受信した第 1 の変換データと 1 または複数の暗号サーバからそれぞれ受信した第 2 の変換データとを用いて、投票者が記述した投票内容を暗号化した暗号投票データを作成する処理と、  
前記暗号投票データ及び前記投票者の認証情報を前記投票サーバまたは認証サーバに送信する処理と、  
を実行させるプログラム。

【請求項 36】

コンピュータに、  
候補者名を暗号化して候補者名とその候補者名を暗号化した暗号投票データとの組のリストを投票機器に送信する処理と、  
認証情報をもとに投票者が有権者であることと未投票であることを確認したのちに前記投票機器または認証サーバからの暗号投票データを受付ける処理と、  
投票期間終了後、既に受信した有効な暗号投票データのリストを匿名復号システムに送信する処理と、  
を実行させるプログラム。

【書類名】明細書

【発明の名称】匿名電子投票システム、匿名電子投票方法およびプログラム

【技術分野】

【0001】

本発明は、匿名電子投票システム、匿名電子投票方法およびプログラムに関し、特に、多様なクライアント環境からも利用可能な匿名電子投票システム、匿名電子投票方法およびプログラムに関する。

【背景技術】

【0002】

匿名電子投票システムは、例えばネットワークなどを介して無記名の秘密投票を電子的に実現するシステムであり、従来の匿名電子投票システムの一例が、特許文献1や非特許文献1に記載されている。なお、以下の説明において、投票には、予め定められている候補者から選挙を行うための投票のみならず、自由記述を許すアンケートなども含まれるものとする。また、候補者や候補者名は、単に選挙における候補者や候補者名を指すものではなく、ある集合から投票者の意思によってある要素あるいは項目を選択する場合のその要素（項目）や要素（項目）名をも含むものである。

【0003】

図28に示すように、従来の匿名電子投票システムは、窓口センタ901と複数の復号シャッフルセンタ902とからなる匿名復号システム900と、各投票者がアクセスすることとなる投票管理センタ（投票サーバ）910と、から構成されている。匿名復号システム900は、投票の秘密を守るために設けられており、暗号データとの対応を秘匿して復号結果を出力するために用いられている。

【0004】

このような構成を有する従来の匿名電子投票システムは、次のように動作する。

【0005】

まず、窓口センタ901と復号シャッフルセンタ902は、投票用の暗号化鍵などのシステムの公開情報を生成して投票管理センタ910に送信し、投票管理センタ910は、各投票者にその公開情報を通知する。

【0006】

投票期間が始まると各投票者は、公開情報に基づいて自分の投票内容を暗号化して暗号投票文を作成し、その暗号投票文に対して投票者のデジタル署名を生成し、暗号投票文とデジタル署名とを投票管理センタ910に送信する。その際、各投票者は、典型的には、自己のクライアント端末において暗号投票文やデジタル署名を作成し、各種のネットワークを介して自己のクライアント端末から投票管理センタ910に対して暗号投票文とデジタル署名とを投票管理センタ910に送信する。投票管理センタ910は、受信したデジタル署名を検証し、有権者名簿をもとに投票者の投票権を確認し、重複投票がないことを確認した後、受信した暗号投票文を受け付ける。

【0007】

投票期間が終わると、投票管理センタ910は、投票の受け付けを終了し、投票開始から終了までに受け付けた暗号投票文のリストを匿名復号システム900の窓口センタ901に送付する。窓口センタ901は、復号シャッフルセンタ902を介して暗号投票文のリストを復号して平文の投票文のリストを得、平文の投票文のリストを投票管理センタ910に返送する。

【0008】

投票管理センタ910は、窓口センタ901から受け取った平文の投票文のリストにより、投票結果の集計を行なう。

【特許文献1】特開2002-237810号公報（図7、[0063]～[0071]）

【特許文献2】特開2001-251289号公報

【特許文献3】特開2002-344445号公報

【非特許文献1】佐古 和恵、外6名、“シャッフリングによる大規模電子投票システムの実現”、情報処理学会第62回全国大会、2001年3月

【発明の開示】

【発明が解決しようとする課題】

【0009】

しかしながら、従来の匿名電子投票システムでは、投票者が使用するクライアント端末が携帯電話機のような記憶容量や処理能力の乏しい機器である場合には、投票の秘密が守られた投票が難しい、という問題点がある。その理由は、従来の匿名電子投票システムで投票者が行なう暗号化処理は記憶容量や処理能力の乏しい機器には実装するのが難しく、一方、他の機器に投票内容を送って暗号化処理を行なうこととすると、暗号化処理を行なう機器には投票内容がわかってしまうからである。

【0010】

また、従来の匿名電子投票システムでは、広く一般の人を有権者とするような投票（例えば公職選挙）において、有権者の認証が困難であり、非有権者の投票や重複投票を防止することが難しい、という問題点もある。その理由は、従来の匿名電子投票システムでは、有権者の認証に利用するデジタル署名において、すべての投票者が共通の公開鍵認証基盤に登録されていることを前提としているが、現在、一般にはそのような基盤が普及していないためである。

【0011】

そこで本発明の目的は、携帯電話機などの記憶容量や処理能力の小さい機器からも投票の秘密を守りつつ投票を行なえる匿名電子投票システム及び匿名電子投票方法を提供することにある。

【0012】

本発明の他の目的は、すべての有権者が共通の公開鍵認証基盤に登録されているような条件が整備されていない場合であっても、有権者認証の行なえる匿名電子投票システム及び匿名電子投票方法を提供することにある。

【課題を解決するための手段】

【0013】

本発明の第1の態様によれば、匿名電子投票システムは、投票者が投票を行うための投票機器と、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、暗号投票データを再度暗号化する再暗号化手段を備え、投票機器から受信した暗号投票データを再度暗号化してその投票機器に返信する暗号サーバと、候補者名とその候補者名を暗号化した暗号投票データとの組のリストを投票機器に送信し、その後、認証情報をもとに投票者が有権者であることと未投票であることを確認したのちに投票機器からの暗号投票データを受付け、受信した有効な暗号投票データのリストを投票期間終了後に匿名復号システムに送信する投票サーバと、を有し、投票機器は、投票サーバからリストを受信した後に、投票者が選択した候補者名に対応する暗号投票データを暗号サーバに送信し、暗号サーバで再度暗号化された暗号投票データを受信して投票サーバに送信するとともに、投票者の認証情報を投票サーバに送信する。

【0014】

上述した本発明の第1の態様に基づいて構成される匿名電子投票システムでは、例えば、投票サーバは匿名復号システムと接続され、投票サーバには暗号化手段を備え、暗号化手段をもたない投票機器は暗号サーバと接続されており、共通基盤署名生成手段をもたない投票機器は認証サーバと接続される。暗号サーバには再暗号化手段を備え、認証サーバにはID連携手段と共通基盤署名生成手段を備える。

【0015】

このような構成を採用し、投票サーバは暗号化手段をもたない投票機器に対しては平文の候補者名と暗号化された候補者名の組を送信し、暗号化手段をもたない投票機器は投票者の選んだ候補者名に対応する、暗号化された候補者名を暗号サーバを介して再度暗号化してから投票サーバに送信し、投票サーバは受信したすべての暗号データを匿名復号シ

テムにより復号する。これにより、本発明の第1の目的を達成することができる。

#### 【0016】

また、共通基盤署名生成手段をもたない投票機器は認証サーバと通信を行なって組織内での個人認証を行ない、認証サーバは組織内に閉じた投票者IDをID連携手段により共通基盤におけるIDに変換し、このIDと投票データの組に認証サーバの共通基盤デジタル署名を付与して投票サーバに送信する。このように、既存の認証基盤を利用して個人認証を行なったことを認証サーバのデジタル署名により証明することで、本発明の第2の目的を達成することができる。

#### 【0017】

本発明の第2の態様によれば、匿名電子投票システムは、投票者が投票を行うための投票機器と、受信した暗号投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する匿名復号システムと、公開情報から第1の変換データを生成する第1の変換手段を備え、第1の変換データを投票機器に送信する投票サーバと、公開情報から第2の変換データを生成する第2の変換手段をそれぞれ備えて第2の変換データを投票機器に送信する1または複数の暗号サーバと、を有し、投票機器は、投票サーバから受信した第1の変換データと各暗号サーバからそれぞれ受信した第2の変換データを用いて、投票者が記述した投票内容を暗号化して暗号投票データを作成して投票サーバに送信し、かつ、投票者の認証情報を投票サーバに送信し、投票サーバは、認証情報をもとに投票者が有権者であることと未投票であることを確認したのちに暗号投票データを受付け、投票期間終了後、既に受信した有効な暗号投票データのリストを匿名復号システムに送信する。

#### 【0018】

上述した本発明の第2の態様に基づいて構成される匿名電子投票システムは、本発明の第1の態様の匿名電子投票システムの投票サーバの暗号化手段にかえて第1の変換手段を備え、暗号サーバの再暗号化手段にかえて第2の変換手段を備え、投票機器に暗号データ作成手段を備えたものである。

#### 【0019】

このような構成を採用し、投票サーバは第1の変換手段により投票内容の暗号化処理に必要な演算の一部を行なって投票機器へ送信し、暗号サーバも同様に第2の変換手段により投票内容の暗号化処理に必要な演算の一部を行なって投票機器へ送信し、投票機器では投票内容とともに、投票サーバから受信した第1の変換結果と暗号サーバから受信した第2の変換結果とを暗号データ作成手段に入力して暗号投票データを作成することで、本発明の第1の目的を達成することができる。

#### 【発明の効果】

#### 【0020】

本発明は、記憶容量や処理能力の小さい機器からも電子投票を行なえる、という効果を有する。その理由は、暗号化処理のすべて、もしくは、暗号化処理のうちで計算量の多い変換処理を、投票機器で行なう必要がないからである。

#### 【0021】

また本発明は、記憶容量や処理能力の小さい機器を使って電子投票を行なっても、投票の秘密を守ることができる、という効果を有する。その理由は、暗号投票データの復号は匿名復号システムによって行なわれるため、すべての暗号投票データが復号されても、どの投票者の暗号投票データがどの平文に対応するかがわからないことと、投票内容の平文は投票サーバと暗号サーバの両方の処理により暗号化され、投票サーバや暗号サーバは単独では投票された暗号投票データを復号できないからである。

#### 【0022】

さらに本発明は、すべての有権者が共通の公開鍵認証基盤に登録されているような条件が整備されていなくても、不正投票を防止しつつ投票を行なえる、という効果を有する。その理由は、組織内に限られた認証手段しかもたない有権者を認証サーバが認証し、その投票データに認証サーバのデジタル署名を付与することで、認証サーバによる投票者の認証が行なわれているデータであることを確認できるからである。

**【発明を実施するための最良の形態】****【0023】**

次に、本発明の好ましい実施の形態について、図面を参照して詳細に説明する。

**【0024】****《第1の実施形態》**

図1は、本発明の第1の実施形態の匿名電子投票システムの構成を示している。この匿名電子投票システムは、それぞれ構成要素や処理能力などが異なっている投票機器100、110、120、130、140、150と、投票センタ（投票管理センタ）200と、認証サーバ300と、暗号サーバ400、410、440と、匿名復号システム500とから構成される。暗号サーバ400、410、440は、それぞれ、投票機器100、110、140と接続している。後述する説明から明らかなように、投票機器100、110、120、130、140、150からの投票センタ200への接続形態は多様であり、あるものは投票センタ200に直接接続し、別のものは認証サーバ300を介して投票センタ200に接続し、また別のものは、直接接続と認証サーバ300を介した接続とを併用している。ここでは簡単のため図示を省略するが、投票機器100、110、120、130、140、150は、それぞれ、複数存在してもかまわない。また、投票機器ひとつにつきひとつの暗号サーバが接続される構成としてもよいし、いくつかの投票機器がひとつの暗号サーバと接続される構成としてもよい。また、暗号サーバと認証サーバとが同一のサーバ上で動作する構成とすることも可能である。

**【0025】**

まず、各投票機器100、110、120、130、140、150の構成について説明する。

**【0026】**

投票機器100は、ディスプレイなどの表示装置101と、ボタンやキーボードなどの入力装置102と、機器側認証手段103とを備え、投票サーバ200、認証サーバ300、暗号サーバ400と通信回線などにより接続されている。

**【0027】**

投票機器110は、ディスプレイなどの表示装置111と、ボタンやキーボードなどの入力装置112と、組織内基盤署名生成手段113とを備え、投票サーバ200、認証サーバ300、暗号サーバ410と通信回線などにより接続されている。

**【0028】**

投票機器120は、ディスプレイなどの表示装置121と、ボタンやキーボードなどの入力装置122と、機器側認証手段123と、暗号化手段124とを備え、投票サーバ200、認証サーバ300と通信回線などにより接続されている。

**【0029】**

投票機器130は、ディスプレイなどの表示装置131と、ボタンやキーボードなどの入力装置132と、組織内基盤署名生成手段133と、暗号化手段134とを備え、投票サーバ200、認証サーバ300と通信回線などにより接続されている。

**【0030】**

投票機器140は、ディスプレイなどの表示装置141と、ボタンやキーボードなどの入力装置142と、共通基盤署名生成手段143とを備え、投票サーバ200、暗号サーバ440と通信回線などにより接続されている。

**【0031】**

投票機器150は、ディスプレイなどの表示装置151と、ボタンやキーボードなどの入力装置152と、共通基盤署名生成手段153と、暗号化手段154とを備え、投票サーバ200と通信回線などにより接続されている。

**【0032】**

投票サーバ200は、有権者名簿データベース201と、共通基盤署名検証手段202と、暗号化手段203と、ハードディスクドライブなどの記録装置204とを備え、投票機器100、110、120、130、140、150及び認証サーバ300と通信回線

などにより接続されている。

【0033】

認証サーバ300は、サーバ側認証手段301と、組織内基盤署名検証手段302と、共通基盤署名生成手段303と、ID連携手段304とを備えている。

【0034】

暗号サーバ400、410、440は、それぞれ再暗号化手段401、411、441を備えている。

【0035】

投票機器100、120の機器側認証手段113、123は、認証サーバ300のサーバ側認証手段301と通信を行ない、投票機器を操作している投票者の識別子がIDjであることの認証を受けるとともに、このサーバ側認証手段301と通信を行ない、投票機器100、120を操作している投票者jの識別子IDjを認証サーバ300に通知する。

【0036】

投票機器120、130、140、150と投票サーバ200とにそれぞれ設けられた暗号化手段124、134、144、154、203は、暗号化公開鍵Yと平文投票データvを入力とし、Yによりvを暗号化した暗号投票データE(v)を出力する。

【0037】

暗号サーバ400、410、440の再暗号化手段401、411、441は、いずれも、暗号化公開鍵Yと暗号投票データE(v)を入力とし、YによりE(v)を再度暗号化した暗号投票データE'(v)を出力する。

【0038】

投票機器110、130の組織内署名生成手段113、133は、暗号投票データE(vj)と投票者jの組織内識別子IIDjと署名用秘密鍵djとを入力とし、(E(vj), IIDj)に対する投票者jの組織内向けデジタル署名Sejを出力する。

【0039】

認証サーバ300の組織内署名検証手段302は、暗号投票データE(vj)と組織内識別子IIDjと組織内向けデジタル署名Sejと検証用公開鍵Pjとを入力とし、Sejが(E(vj), IIDj)に対して署名用秘密鍵djにより正しく計算されたものかどうかを判定する。

【0040】

投票機器140、150の共通基盤署名生成手段143、153は、暗号投票データE(vj)と投票者jの共通識別子CIDjと署名用秘密鍵djを入力とし、(E(vj), CIDj)に対する投票者jの共通基盤デジタル署名Sekを出力する。

【0041】

認証サーバ300の共通基盤署名生成手段303は、暗号投票データE(vj)と投票者jの共通識別子CIDjと、認証サーバの署名用秘密鍵dkを入力とし、(E(vj), CIDj)に対する認証サーバの共通基盤デジタル署名Sekを出力する。

【0042】

投票センタ200の共通基盤署名検証手段202は、暗号投票データE(vj)と共通識別子CIDjと共通基盤デジタル署名Sekを入力とし、Sekが(E(vj), CIDj)に対して署名用秘密鍵dkにより正しく計算されたものかどうかを判定する。

【0043】

認証サーバ300のID連携手段304には、組織内識別子IIDjと共通識別子CIDjとの対応関係が記録されており、組織内識別子IIDjを入力されると対応する共通識別子CIDjを出力する。

【0044】

匿名復号システム500は、外部から入力された初期設定情報に従って暗号化公開鍵Yを生成して出力し、外部から暗号投票データE(vj)のリストを入力されると、E(vj)のリストを復号し、順番をランダムに並びかえた平文投票データvjのリストと、入

力された  $E(v_j)$  のリストと出力した  $v_j$  のリストとの間に 1 対 1 の対応関係があることの証明データとを出力する。

#### 【0045】

投票機器 110, 130 の組織内署名生成手段 113, 133 と、投票機器 140, 150 の共通基盤署名生成手段 143, 153 と、認証サーバ 300 の共通基盤署名生成手段 303 は、いずれもデジタル署名を作成するものであり、これに対し認証サーバ 300 の組織内署名検証手段 302 と投票サーバ 200 の共通基盤署名検証手段 202 とは、デジタル署名の検証を行うものである。ここでのデジタル署名には、例えば RSA 暗号などの公開鍵暗号を用いるデジタル署名を用いることができる。RSA 暗号を用いる場合、署名者  $j$  のデータ  $V$  に対する署名  $S_{jv}$  は、 $V$  と署名者  $j$  の署名用秘密鍵  $d_j$  を用いて、

$$S_{jv} = V^{d_j} \bmod n$$

により計算され、署名検証は、 $V$  と  $S_{jv}$  と、 $d_j$  に対応する検証用公開鍵  $e_j$  を用いて、

$$S_{jv}^{e_j} = V \bmod n$$

が成り立てば合格となる。なお、 $^{\wedge}$  はべき乗を表わす記号であり、 $V^{d_j}$  は  $V$  を  $d_j$  回べき乗した結果（すなわち  $V^{d_j}$ ）を表わす。

#### 【0046】

ここで、 $d_j, e_j, n$  は、二つの素数  $p, q$  に対して、

$$n = p \times q,$$

$$d_j \times e_j = 1 \bmod (p-1) \times (q-1)$$

と表わされる整数であり、あらかじめ各署名者  $j$  ごとに相異なる  $(d_j, e_j)$  の組を作成し、 $d_j$  は各署名者  $j$  が秘密に保持し、 $(n, e_j)$  の組は署名者  $j$  の識別子  $ID_j$  と関連づけて公開しておくようにする。署名検証においては、公開されている  $ID_j$  と  $(n, e_j)$  との対応関係を検索して  $(n, e_j)$  を取得して署名検証の処理を行なう。 $d_j$  は署名生成用秘密鍵、 $(n, e_j)$  は署名検証用公開鍵とよばれる。

#### 【0047】

組織内署名生成手段 113, 133 及び組織内署名検証手段 302 においては、識別子  $ID_j$  は例えば社員番号など、ある組織の内部でのみ公開・利用される組織内識別子であり、別々の組織に属する別の個人に割り振られた識別子が同じ  $ID_j$  になっている可能性もあり、また、有権者名簿に登録される有権者の識別子（有権者名など）との対応関係は公開されているとは限らない。 $ID_j$  に対応する署名検証用公開鍵  $(n, e_j)$  の組も同様に、組織の内部にのみ公開される場合もある。

#### 【0048】

一方、共通基盤署名生成手段 143, 153, 303 及び共通基盤署名検証手段 202 においては、署名者の識別子  $ID_j$  と  $(n, e_j)$  とは広く一般に公開され、別の個人に同じ識別子が割り振られることのない、共通識別子であり、有権者名簿データベース 201 には共通識別子を含む情報が記録される。

#### 【0049】

投票機器 100, 120 の機器側認証手段 103, 123 と、認証サーバ 300 のサーバ側認証手段 301 は、個人認証を行うものである。ここでは、ID 文字列とパスワードによる個人認証や、携帯電話の端末認証に基づいた個人認証などを用いることができる。

#### 【0050】

ID 文字列とパスワードによる個人認証を行なう場合、認証サーバ 300 にはあらかじめ投票者の組織内識別子とパスワードの対応関係を記録しておく。機器側認証手段 103, 123 は、入力装置 102, 122 から入力された投票者の組織内識別子  $IID_j$  を認証サーバ 300 に送る。認証サーバ 300 は、サーバ側認証手段 301 により、受信した  $IID_j$  があらかじめ記録された組織内識別子のリストに含まれることを確認し、乱数  $c$  を生成して投票機器 100, 120 へ返信する。機器側認証手段 103, 123 は、入力装置 102, 122 から入力されたパスワード  $pw$  と乱数  $c$  とを SHA1 などのハッシュ関数に入力し、出力された値  $r$  を認証サーバ 300 に返信する。サーバ側認証手段 301

は、あらかじめ記録された組織内識別子とパスワードのリストを  $IID_j$  をキーとして検索し、 $IID_j$  に対応する  $pw$  を取得し、SHA1などのハッシュ関数に  $pw$  と  $c$  とを入力し、出力された値が投票機器 100, 120 から返信された  $r$  と一致すれば、投票機器 100, 120 を操作している投票者を  $IID_j$  で示される投票者であると認める。

#### 【0051】

本実施形態において、投票機器 120, 130, 150 及び投票サーバ 200 に設けられる暗号化手段 123, 133, 153, 203 と、暗号サーバ 400, 410, 440 に設けられる再暗号化手段 401, 411, 441 と、匿名復号システム 500 については、例えば特許文献 1 に示された技術を用いることができる。

#### 【0052】

特許文献 1 に示された技術を用いる場合、匿名復号システム 500 は、投票センタ 200 からセキュリティパラメータ ( $p, q, t$ ) とセッション ID を入力されると、( $p, q, t$ ) に従って公開情報 ( $p, q, g$ ) と秘密鍵  $X$  を生成し、公開情報に公開鍵  $Y$  を加えた公開情報 ( $p, q, g, Y$ ) を出力して投票センタ 200 に返信する。ここで、 $p, q$  はエルガマル暗号のパラメータであり、ある整数  $k$  により

$$p = k \times q + 1$$

という関係にある素数である。 $g$  は、法  $p$  における位数  $q$  の部分群を生成する生成元である。また、 $p, q$  は、素数  $p, q$  の長さであり、 $t$  は、順番入れ替え処理が正しいことを証明するためにデータの生成時および検証時に使用する繰り返し回数である。セッション ID は処理対象を識別するための識別子である。ここで、処理対象は、例えば県知事選挙、市議会議員選挙などである。公開鍵  $Y$  は復号鍵  $X$  に対して、

$$Y = g^X \mod q$$

の計算によって得られた値であり、復号鍵  $X$  は無作為に選ばれた  $q$  未満の乱数である。

#### 【0053】

暗号化手段 123, 133, 153, 203 は、公開情報 ( $p, q, g, Y$ ) と平文投票データ  $v_i$  を入力とし、暗号投票データ  $E(v_i)$  を出力する。 $E(v_i)$  は ( $G_i, V_i$ ) という組で表され、

$$(G_i, V_i) = (g^r \mod p, v_i \times Y^r \mod p)$$

の計算によって得られる。ここで  $r$  は、平文投票データ  $v_i$  に対して無作為に選んだ乱数である。

#### 【0054】

なお本実施形態においては、このとき、正しく  $r$  を知って暗号投票データを作成したことの証明を作成することができる。例えば、 $v_i$  の暗号化において乱数  $s_i$  を生成し、

$$\alpha_i = g^{s_i} \mod p,$$

$$c_i = \text{HASH}(p, q, g, Y, G_i, V_i, \alpha_i),$$

$$t_i = c_i \times r_i + s_i \mod p$$

により、乱数証明データ  $\alpha_i, t_i$  を生成する。この証明は、

$$c_i = \text{HASH}(p, q, g, G_i, \alpha_i)$$

を計算し、

$$g^{t_i} \times G_i^{-c_i} = \alpha_i \mod p$$

が成り立つかどうかを確認することで検証できる。ここで、 $\text{HASH}(p, q, g, Y, G_i, V_i, \alpha_i)$  は SHA1 などのハッシュ関数に  $p, q, g, Y, G_i, V_i, \alpha_i$  を入力して得られる値である。

#### 【0055】

再暗号化手段 401, 411, 441 は、公開情報 ( $p, q, g, Y$ ) と暗号投票データ  $E(v_i) = (G_i, V_i)$  を入力とし、暗号投票データ  $E'(v_i)$  を出力する。 $E'(v_i)$  は ( $G'_i, V'_i$ ) という組で表され、

$$(G'_i, V'_i) = (G_i \times g^s \mod p, V_i \times Y^s \mod p)$$

の計算によって得られる。ここで、 $s$  は暗号投票データ  $E(v_i)$  に対して無作為に選んだ乱数である。なお、

$$(G' i, V' i) = (G i \times g^s \bmod p, V i \times Y^s \bmod p) \\ = (g^{\{r+s\}} \bmod p, v i \times Y^{\{r+s\}} \bmod p)$$

の等式が成り立っており、 $E(v i)$  に対する復号処理と同じ処理を  $E'(v i)$  に施すことで平文投票データ  $v i$  を得ることができる。つまり、 $E(v i)$  と  $E'(v i)$  とは復号処理に関しては同様に扱える。

#### 【0056】

投票センタ200が  $E i = (G i, V i)$  のリストとセッションIDを匿名復号システム500に入力すると、匿名復号システム500は、セッションIDにより特定された公開情報  $(p, q, g, Y)$  および復号鍵  $X$  により  $(G i, V i)$  のリストを復号し、順番をランダムに並びかえた平文投票データ  $v i$  のリストと、 $(G i, V i)$  のリストと  $v i$  のリストとの間に1対1の対応関係があることの証明データを投票センタ200に返信する。

#### 【0057】

$p, q, g, X$  の生成、 $(G i, V i)$  のリストの復号と順番の並べかえ、 $(G i, V i)$  のリストと  $v i$  との間に1対1の対応関係があることの証明とその検証方法については、特許文献1に記載の方法を用いる。

#### 【0058】

ここでは、特許文献1の技術を用いる場合の、主に各構成要素の入出力について説明した。なお、暗号データのリストを、復号後に出力されるデータリストとの間に1対1の対応関係があることを、具体的な対応関係そのものの情報は一切漏らさずに証明する技術は、特開2001-251289号公報（特許文献2）、特開2002-344445号公報（特許文献3）などにも示されており、これらの技術を用いて暗号化手段123, 133, 153, 再暗号化手段401, 411, 441、匿名復号システム500を実現することも可能である。

#### 【0059】

次に、本実施形態の匿名電子投票システムの全体の動作について説明する。

#### 【0060】

図2には、この匿名電子投票システムでの初期設定の動作が記述されている。まず、投票サーバ200は、セキュリティパラメータ  $(p, q, g, Y)$  とセッションIDとを匿名復号システム500に送信する（ステップA1）。匿名復号システム500は、 $(p, q, g, Y)$  にしたがって公開情報  $(p, q, g, Y)$  を作成し（ステップA2）、投票サーバ200へ返信する（ステップA3）。投票サーバ200は、 $(p, q, g, Y)$  を記録装置204に記録する（ステップA4）。以上により、初期設定が終了する。

#### 【0061】

次に、図3～図9を参照して、投票機器100, 110, 120, 130, 140, 150を使った投票の動作を説明する。ここで、図3～図8は、それぞれ、投票機器100, 110, 120, 130, 140, 150での処理（及びそれらの投票機器での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理）を示している。また、図9は、投票受付後から開票に相当する作業までの処理を説明している。

#### 【0062】

投票期間が始まると、有権者である投票者は、投票機器100, 110, 120, 130, 140, 150のいずれかにより投票サーバ200へアクセスする。このとき、投票機器100, 110, 140からの投票では暗号投票情報要求を送信し（図3、図4、図7のステップA5-1）、投票機器120, 130, 150からの投票では単なる投票情報要求を送信する（図5、図6、図8のステップA5-2）。投票サーバ200は、投票機器100, 110, 140からの暗号投票情報要求を受信すると、その暗号化手段203により、すべての候補者名  $v j$  を公開情報  $(p, q, g, Y)$  で暗号化することによって  $(v j, E(v j))$  のリストを作成し（図3、図4、図7のステップA6）、公開情報  $(p, q, g, Y)$  と  $(v j, E(v j))$  のリストとを投票機器100, 110, 140に返信する（図3、図4、図7のステップA7-1）。また、投票機器120, 130

0, 150からの単なる投票情報要求を受信すると、投票サーバ200は、公開情報(p, q, g, Y)と平文の候補者名 $v_j$ のリストとを投票機器120, 130, 150に返信する(図5、図6、図8のステップA7-2)。

**【0063】**

以下、投票データの送信までの処理を、投票機器100, 110, 120, 130, 140, 150ごとに別々に説明する。

**【0064】**

投票機器100は、図3に示すように、(p, q, g, Y)と( $v_j$ , E( $v_j$ ))のリストとを受信すると、その表示装置101において $v_j$ のリストを投票者に対して表示し、投票者は入力装置102により $v_j$ のリストから候補者名 $v_i$ を選択して入力する(ステップA100-1)。そして投票機器100は、 $v_i$ に対応するE( $v_i$ )と公開情報(p, q, g, Y)とを暗号サーバ400に送信する(ステップA100-2)。次に、暗号サーバ400は、受信したE( $v_i$ )と公開情報(p, q, g, Y)とを再暗号手段401に入力してE( $v_i$ )を再度暗号化したE'( $v_i$ )を計算し(ステップA100-3)、E'( $v_i$ )を投票機器100に返信する(ステップA100-4)。次に、投票機器100は、入力装置102により投票者の組織内識別子IID $_i$ を取得し、機器側認証手段103により認証サーバ300に対して投票者 $i$ の組織内識別子IID $_i$ の認証を行ない(ステップA100-5)、E'( $v_i$ )を認証サーバ300に送信する(ステップA100-6)。

**【0065】**

認証サーバ300は、サーバ側認証手段301により確認した投票者の組織内識別子IID $_i$ をID連携手段304に入力し、対応する共通識別子CID $_i$ を得る(ステップA100-7)。次に、認証サーバ300では、共通基盤署名生成手段303に(E'( $v_i$ ), CID $_i$ )の組と認証サーバ300の署名用秘密鍵dkとが入力されて、(E'( $v_i$ ), CID $_i$ )に対する認証サーバ300の共通基盤署名Sekが生成される(ステップA100-8)。そして、認証サーバ300は、(E $_i$ , CID $_i$ ) = (E'( $v_i$ ), CID $_i$ )とSekとを投票サーバ200に送信する(ステップA100-9)。

**【0066】**

投票機器110は、図4に示すように、(p, q, g, Y)と( $v_j$ , E( $v_j$ ))のリストとを受信すると、その表示装置111において $v_j$ のリストを投票者に対して表示し、投票者は入力装置112により $v_j$ のリストから候補者名 $v_i$ を選択して入力する(図4のステップA110-1)。そして、投票機器110は、 $v_i$ に対応するE( $v_i$ )と公開情報(p, q, g, Y)とを暗号サーバ410に送信する(図4のステップA110-2)。暗号サーバ410は、受信したE( $v_i$ )と公開情報(p, q, g, Y)とを再暗号手段411に入力してE( $v_i$ )を再度暗号化したE'( $v_i$ )を計算し(ステップA110-3)、E'( $v_i$ )を投票機器110に返信する(ステップA110-4)。次に、投票機器110は、組織内署名生成手段113に投票者 $i$ の組織内識別子IID $_i$ と署名用秘密鍵diとE'( $v_i$ )とを入力し、(E'( $v_i$ ), IID $_i$ )に対する組織内向けデジタル署名Se $_i$ を計算し(ステップA110-5)、(E'( $v_i$ ), IID $_i$ )とSe $_i$ とを認証サーバ300に送信する(ステップA110-6)。

**【0067】**

認証サーバ300は、その組織内署名検証手段302により、Se $_i$ が(E'( $v_i$ ), IID $_i$ )に対して署名用秘密鍵diにより正しく計算されたものかどうかを検証し(ステップA110-7)、合格であれば、ID連携手段304によってIID $_i$ に対応する共通識別子CID $_i$ を取得する(ステップA110-8)。次に、認証サーバ300は、共通基盤署名生成手段303にE'( $v_i$ )とCID $_i$ と認証サーバ300の署名用秘密鍵dkとを入力して、(E'( $v_i$ ), CID $_i$ )に対する認証サーバ300の共通基盤デジタル署名Sekを出力し(ステップA110-9)、(E $_i$ , CID $_i$ ) = (E'( $v_i$ ), CID $_i$ )とSekとを投票サーバ200に送信する(ステップA110-10)。

## 【0068】

投票機器120は、図5に示すように、 $(p, q, g, Y)$ と $v_j$ のリストとを受信すると、その表示装置121において $v_j$ のリストを投票者に対して表示し、投票者は入力装置122により $v_j$ のリストから候補者名 $v_i$ を選択して入力する(ステップA120-1)。そして投票機器120は、 $v_i$ と公開情報 $(p, q, g, Y)$ とを暗号化手段124に入力し、 $v_i$ を $Y$ により暗号化した $E(v_i)$ を得る(ステップA120-2)。次に、投票機器120は、機器側認証手段123により認証サーバ300に対して投票者 $i$ の組織内識別子 $IID_i$ の認証を行ない(ステップA120-3)、 $E(v_i)$ を認証サーバ300に送信する(ステップA120-4)。

## 【0069】

認証サーバ300は、サーバ側認証手段301により確認した投票者の組織内識別子 $IID_i$ をID連携手段304に入力し、対応する共通識別子 $CID_i$ を得る(ステップA120-5)。次に、認証サーバ300は、共通基盤署名生成手段303に $(E(v_i), CID_i)$ の組と認証サーバ300の署名用秘密鍵 $dk$ を入力して、 $(E(v_i), CID_i)$ に対する共通基盤署名 $Se_k$ を生成し(ステップA120-6)、 $(E_i, CID_i) = (E(v_i), CID_i)$ と $Se_k$ とを投票サーバ200に送信する(ステップA120-7)。

## 【0070】

投票機器130は、図6に示すように、 $(p, q, g, Y)$ と $v_j$ のリストとを受信すると、その表示装置131において $v_j$ のリストを投票者に対して表示し、投票者は入力装置132により $v_j$ のリストから候補者名 $v_i$ を選択して入力する(ステップA130-1)。そして投票機器130は、 $v_i$ と公開情報 $(p, q, g, Y)$ とを暗号化手段134に入力し、 $v_i$ を $Y$ により暗号化した $E(v_i)$ を得る(ステップA130-2)。次に投票機器130は、組織内署名生成手段133に投票者 $i$ の組織内識別子 $IID_i$ と署名用秘密鍵 $d_i$ と $E(v_i)$ とを入力し、 $(E(v_i), IID_i)$ に対する組織内向けデジタル署名 $Se_i$ を計算し(ステップA130-3)、 $(E(v_i), IID_i)$ と $Se_i$ とを認証サーバ300に送信する(ステップA130-4)。

## 【0071】

認証サーバ300は、組織内署名検証手段302により、 $Se_i$ が $(E(v_i), IID_i)$ に対して署名用秘密鍵 $d_i$ により正しく計算されたものかどうか検証し(ステップA130-5)、合格であれば、ID連携手段304により $IID_i$ に対応する共通識別子 $CID_i$ を取得する(ステップA130-6)。次に認証サーバ300は、共通基盤署名生成手段303に $E(v_i)$ と $CID_i$ と認証サーバ300の署名用秘密鍵 $dk$ とを入力して、 $(E(v_i), CID_i)$ に対する認証サーバ300の共通基盤デジタル署名 $Se_k$ を出力し(ステップA130-7)、 $(E_i, CID_i) = (E(v_i), CID_i)$ と $Se_k$ とを投票サーバ200に送信する(ステップA130-8)。

## 【0072】

投票機器140は、図7に示すように、 $(p, q, g, Y)$ と $(v_j, E(v_j))$ のリストとを受信すると、その表示装置141において $v_j$ のリストを投票者に対して表示し、投票者は入力装置142により $v_j$ のリストから候補者名 $v_i$ を選択して入力する(ステップA140-1)。そして投票機器140は、 $v_i$ に対応する $E(v_i)$ と公開情報 $(p, q, g, Y)$ とを暗号サーバ440に送信する(ステップA140-2)。次に暗号サーバ440は、受信した $E(v_i)$ と公開情報 $(p, q, g, Y)$ とを再暗号手段441に入力して $E(v_i)$ を再度暗号化した $E'(v_i)$ を計算し(ステップA140-3)、 $E'(v_i)$ を投票機器140に返信する(ステップA140-4)。次に投票機器140は、共通基盤署名生成手段143に投票者 $i$ の共通基盤識別子 $CID_i$ と署名用秘密鍵 $d_i$ と $E'(v_i)$ とを入力し、 $(E'(v_i), CID_i)$ に対する共通基盤デジタル署名 $Se_i$ を計算し(ステップA140-5)、 $(E_i, CID_i) = (E'(v_i), CID_i)$ と $Se_i$ とを投票サーバ200に送信する(ステップA140-6)。

。

**【0073】**

投票機器150は、図8に示すように、 $(p, q, g, Y)$ と $v_j$ のリストとを受信すると、表示装置151において $v_j$ のリストを投票者に対して表示し、投票者は入力装置152により $v_j$ のリストから候補者名 $v_i$ を選択し入力する(ステップA150-1)。そして投票機器150は、 $v_i$ と公開情報 $(p, q, g, Y)$ とを暗号化手段154に入力して $v_i$ を $Y$ により暗号化した $E(v_i)$ を得る(ステップA150-2)。次に投票機器150は、共通基盤署名生成手段153に投票者 $i$ の共通基盤識別子 $CID_i$ と署名用秘密鍵 $d_i$ と $E(v_i)$ とを入力し、 $(E(v_i), CID_i)$ に対する共通基盤デジタル署名 $Se_i$ を計算し(ステップA150-3)、 $(E_i, CID_i) = (E(v_i), CID_i)$ と $Se_i$ とを投票サーバ200に送信する(ステップA150-4)。

**【0074】**

以上が、投票データの送信までの処理である。つづいて、投票データの受け付けと投票締切後の開票集計処理について、図9を用いて説明する。

**【0075】**

投票サーバ200は、認証サーバ300から $(E_i, CID_i)$ と $Se_k$ とを受信すると、共通基盤署名検証手段202により $Se_k$ が $(E_i, CID_i)$ に対する認証サーバ300の正しい署名であることを確認し(ステップA8-1)、有権者名簿データベース201を検索して $CID_i$ が登録されていることと $CID_i$ の投票をまだ受付けていないことを確認し(ステップA9-1)、投票データ記録装置204に $(E_i, CID_i)$ と $Se_k$ とを記録するとともに、有権者名簿データベース201に $CID_i$ が投票済みであることを記録する(ステップA10-1)。また、投票サーバ200は、投票機器140, 150から $(E_i, CID_i)$ と $Se_i$ とを受信すると、共通基盤署名検証手段202により $Se_i$ が $(E_i, CID_i)$ に対する投票者 $i$ の正しい署名であることを確認し(ステップA8-2)、有権者名簿データベース201を検索して $CID_i$ が登録されていることと $CID_i$ の投票をまだ受付けていないことを確認し(ステップA9-2)、投票データ記録装置204に $(E_i, CID_i)$ と $Se_k$ とを記録するとともに、有権者名簿データベース201に $CID_i$ が投票済みであることを記録する(ステップA10-2)。

**【0076】**

投票が締め切られた後、投票サーバ200は、投票データ記録装置204に記録したすべての $E_i$ のリストと、ステップA2で匿名復号システム500へ送信したセッションIDとを匿名復号システム500へ送信する(ステップA11)。匿名復号システム500は、セッションIDで指定された公開情報 $(p, q, g, Y)$ と秘密鍵 $X$ とに基づいて $E_i$ のリストを復号し、順番を無作為に並べかえた平文投票データ $v_j$ のリストと、 $E_i$ のリストと $v_j$ のリストとの間に1対1の対応関係が存在することの証明データ $z$ と、を作成し(ステップA12)、投票サーバ200に対して $v_j$ のリストと $z$ とを返信する(ステップA13)。投票サーバ200は、受信した平文投票データ $v_j$ のリストにより投票の集計を行い、集計結果を発表する(ステップA14)。

**【0077】**

次に、本実施形態の効果について説明する。

**【0078】**

本実施形態では、投票サーバ200が投票機器100, 110, 140に暗号投票データを送り、投票者が選んだ暗号投票データを暗号サーバ400, 410, 440によりさらに暗号化して投票サーバ200に送信するため、暗号手段を備えない投票機器からでも、投票の秘密を守りつつ、投票を行なえる。また、投票機器100, 120に機器側認証手段103, 123を備え、認証サーバ300にサーバ側認証手段301を備えることでデジタル署名に依らない認証を行ない、認証サーバ300の共通基盤デジタル署名を付与して投票サーバ200に暗号投票データを送ることで、署名生成手段を備えない投票機器からも投票を行なえる。また、投票機器110, 130に組織内基盤署名生成手段113, 133を備え、認証サーバ300に組織内基盤署名検証手段302とID連携手段30

4を備えることで、組織内向けデジタル署名が付与された暗号投票データを認証サーバ300で検証し、組織内識別子から共通基盤識別子への変換を行なったのち、認証サーバ300の共通基盤デジタル署名を付与して投票サーバ200へ送ることで、すべての投票者が共通の公開鍵認証基盤に登録されていなくとも、投票を行なえる。

#### 【0079】

なお、ここでは認証サーバ300はひとつだけとして説明したが、投票者によって異なる組織に所属している場合には、組織ごとに別の認証サーバを導入することで対応が可能である。

#### 【0080】

##### 《第2の実施形態》

次に、本発明の第2の実施形態について図面を参照して説明する。図10に示した第2の実施形態の匿名電子投票システムは、図1に示された第1の実施形態の匿名電子投票システムにおいて、投票機器100、110、140内にそれぞれ暗号データ作成手段104、114、144を設けるとともに、投票サーバ200の暗号化手段203に代えて第1の変換手段206と暗号化証明検証手段207とを設け、暗号サーバ400、410、440における再暗号化手段401、411、441に代えてそれぞれ第2の変換手段405、415、445を設け、さらに、変換検証手段701を備える変換検証サーバ700を加えたものである。

#### 【0081】

ここで第1の変換手段206は、公開情報を入力とし、第1の変換データと第1の変換証明データを出力するものである。

#### 【0082】

第2の変換手段405、415、445は、公開情報を入力とし、第2の変換データと第2の変換証明データを出力する。

#### 【0083】

暗号データ作成手段104、114、144は、公開情報と、第1の変換データ、第1の変換証明データ、第2の変換データ、第2の変換証明データ及び平文の投票内容  $v_i$  とを入力として、暗号投票データ  $E(v_i)$  を出力するとともに、 $E(v_i)$  を正しく生成したことを証明する暗号化証明を出力する。

#### 【0084】

暗号化証明検証手段207は、公開情報と暗号投票データ  $E(v_i)$  と暗号化証明データとを入力とし、 $E(v_i)$  が正しく生成されたものかどうかを検証する。

#### 【0085】

第1の変換手段206、第2の変換手段405、415、445、暗号データ作成手段104、114、144及び暗号化証明検証手段207は、匿名復号システム500に対して特許文献1に示された技術を用いる場合、以下のように動作する。

#### 【0086】

第1の変換手段206は、公開情報  $(p, q, g, Y)$  を入力されると、 $q$  未満の乱数  $r$  と  $d$  とを無作為に選び、第1の変換データ  $(G_r, Y_r, r)$  として、

$$(G_r, Y_r, r) = (g^r \bmod p, Y^r \bmod p, r)$$

を計算して出力し、第1の変換証明データ  $(G_d, d)$  として、

$$(G_d, d) = (g^d \bmod p, d)$$

を計算して出力する。

#### 【0087】

第2の変換手段405、415、445は、公開情報  $(p, q, g, Y)$  を入力されると、 $q$  未満の乱数  $s$  を選び、第2の変換データ  $(G_s, Y_s, s)$  として、

$$(G_s, Y_s, s) = (g^s \bmod p, Y^s \bmod p, s)$$

を計算して出力し、第2の変換証明データ  $(G_u, u)$  として、

$$(G_u, u) = (g^u \bmod p, u)$$

を計算して出力する。ここで、 $u$  は無作為に選んだ  $q$  未満の乱数である。

## 【0088】

暗号データ作成手段は、第1の変換データ ( $G_r, Y_r, r$ )、第1の変換証明データ ( $G_d, d$ )、第2の変換データ ( $G_s, Y_s, s$ )、第2の変換証明データ ( $G_u, u$ ) 及び平文の投票内容  $v_i$  とを入力されると、暗号投票データ  $E(v_i)$  として、

$E(v_i) = (G_r \times G_s \bmod p, v_i \times Y_r \times Y_s \bmod p)$   
を計算する。さらに、

$$\alpha = G_u \times G_d \bmod p,$$

$$c = \text{HASH}(p, q, g, Y, G_i, V_i, \alpha),$$

$$t = c \times (r + s) + u + d \bmod q$$

を計算して暗号化証明データ ( $\alpha, t$ ) を計算し、暗号投票データ ( $G_i, V_i$ ) とともにこの暗号化証明データ ( $\alpha, t$ ) を出力する。

## 【0089】

この証明は、暗号化証明検証手段207により

$$c = \text{HASH}(p, q, g, Y, G_i, V_i, \alpha)$$

を計算し、

$$g^t \times G_i^{-c} = \alpha \bmod p$$

が成り立つかどうかを確認することで検証できる。

## 【0090】

変換検証手段701は変換データ ( $G_r, Y_r, r$ ) と変換証明データ ( $G_d, d$ ) について、公開情報 ( $p, q, g, Y$ ) から正しく作成されたものかどうかを検証する。匿名複号システム500に対して特許文献1に示された技術を用いる場合、変換検証手段701は公開情報 ( $p, q, g, Y$ ) と変換データ ( $G_r, Y_r, r$ ) と変換証明データ ( $G_d, d$ ) とを入力とし、

$$G_r = G^r \bmod p,$$

$$Y_r = Y^r \bmod p,$$

$$G_d = Y^d \bmod p$$

の等式がいずれも成り立てば合格と判定し、どれかひとつでも成り立たなければ不合格と判定する。

## 【0091】

次に、本実施形態の匿名電子投票システムの動作について説明する。図11～図13は、それぞれ、投票機器100、110、140での処理（及びそれらの投票機器での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理）を示しており、図14は、投票受付後から開票に相当する作業までの処理を説明している。なお、本実施形態での初期設定の動作は第1の実施の形態と同じであり、また、投票機器120、130、150の動作も第1の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

## 【0092】

以下、投票機器100、110、140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

## 【0093】

投票機器100、110、140は、投票情報要求と変換データ要求とを投票サーバ200へ送信する（図11、図12、図13のステップB5）。投票サーバ200は、変換データ要求を受信すると、その第1の変換手段206に公開情報 ( $p, q, g, Y$ ) を入力し、第1の変換データ ( $G_r, Y_r, r$ ) と第1の変換証明データ ( $G_d, d$ ) とを作成し（図11、図12、図13ステップB6）、投票機器100、110、140にこれら ( $p, q, g, Y$ )、( $G_r, Y_r, r$ )、( $G_d, d$ ) を返信する（図11、図12、図13のステップB7）。投票機器100、110、140は、投票サーバ200から ( $p, q, g, Y$ )、( $G_r, Y_r, r$ )、( $G_d, d$ ) を受信すると、それぞれ暗号サーバ400、410、440に、( $p, q, g, Y$ ) と変換データ要求とを送信する（図11、図12、図13のステップB100-1、B110-1、B140-1）。暗号サ

ーバ400, 410, 440は、公開情報(p, q, g, Y)と変換データ要求とを受信すると、それぞれその第2の変換手段405, 415, 445に(p, q, g, Y)を入力して第2の変換データ(Gs, Ys, s)と第2の変換証明データ(Gu, u)とを生成し(図11、図12、図13のステップB100-2、B110-2、B140-2)、投票機器100, 110, 140に(Gs, Ys, s)と(Gu, u)とを返信する(図11、図12、図13のステップB100-3, B110-3, B140-3)。

**【0094】**

以下、投票データの送信までの処理のうち第1の実施の形態と異なる部分を、投票機器100, 110, 140ごとに別々に説明する。

**【0095】**

投票機器100は、図11に示すように、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)及び第2の変換証明データ(Gu, u)を受信すると、その暗号データ作成手段104に対して、投票者iが入力した投票内容viと、(Gr, Yr, r), (Gd, d), (Gs, Ys, s)及び(Gu, u)とを入力し、暗号投票データE(vi)と暗号化証明データ(α, t)とを計算する(ステップB100-4)。そしてIIDiの認証ののちE(vi)と(α, t)とを認証サーバ300に送信する(ステップB100-6)。認証サーバ300は、(E(vi), (α, t), CIDi)に対する認証サーバ300の共通基盤デジタル署名Sekを作成し(ステップB100-8)、(E(vi), (α, t), CIDi)とSekとを投票サーバ200に送信する(ステップB100-9)。

**【0096】**

投票機器110は、図12に示すように、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)及び第2の変換証明データ(Gu, u)を受信すると、投票者iが入力した投票内容viと、(Gr, Yr, r), (Gd, d), (Gs, Ys, s)及び(Gu, u)とを暗号データ作成手段114に入力し、暗号投票データE(vi)と暗号化証明データ(α, t)とを計算する(ステップB110-4)。そして、投票機器110は、(E(vi), (α, t), IIDi)に対する組織内向けデジタル署名Seiを作成し(ステップB110-5)、(E(vi), (α, t), IIDi)とSeiとを認証サーバ300に送信する(ステップB110-6)。認証サーバ300は、Seiが(E(vi), (α, t), IIDi)に対するIIDiの正しい署名であることを確認し(ステップB110-7)、そのID連携手段304によりIIDiに対応する共通識別子CIDiを取得し(ステップA110-8)、(E(vi), (α, t), CIDi)に対する認証サーバ300の共通基盤デジタル署名Sekを作成し(ステップB110-9)、(Ei=E(vi), (α, t), CIDi)とSekとを投票サーバ200に送信する(ステップB110-10)。

**【0097】**

投票機器140は、図13に示すように、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)及び第2の変換証明データ(Gu, u)を受信すると、投票者iが入力した投票内容viと(Gr, Yr, r), (Gd, d), (Gs, Ys, s)及び(Gu, u)とを暗号データ作成手段144に入力し、暗号投票データE(vi)と暗号化証明データ(α, t)とを計算する(ステップB140-4)。そして、(E(vi), (α, t), CIDi)に対する共通基盤デジタル署名Seiを作成し(ステップB140-5)、(Ei=E(vi), (α, t), CIDi)とSeiとを投票サーバ200に送信する(ステップB140-6)。

**【0098】**

以上が投票データの送信までの処理である。続けて、投票データの受付け以降の処理について、図14を用いて、第1の実施の形態と異なる部分を説明する。

**【0099】**

投票サーバ200は、認証サーバ300から(Ei, (α, t), CIDi)とSekとを受信すると、共通基盤署名検証手段202によりSekが(Ei, CIDi)に対す

る認証サーバ300の正しい署名であることを確認し(ステップB8-1)、暗号化証明検証手段207により、 $E_i$ が正しく作られたものであることを確認し(ステップB9-1)、有権者名簿データベース201を検索して $CID_i$ が登録されていることと $CID_i$ の投票をまだ受付けていないことを確認し(ステップB10-1)、投票データ記録装置204に $(E_i, (\alpha, t), CID_i)$ と $Se_k$ とを記録するとともに、有権者名簿データベース201に $CID_i$ が投票済みであることを記録する(ステップB11-1)。また、投票サーバ200は、投票機器140, 150から $(E_i, (\alpha, t), CID_i)$ と $Se_i$ とを受信すると、共通基盤署名検証手段202により $Se_i$ が $(E_i, (\alpha, t), CID_i)$ に対する投票者 $i$ の正しい署名であることを確認し(ステップB8-2)、暗号化証明検証手段207により、 $E_i$ が正しく作られたものであることを確認し(ステップB9-2)、有権者名簿データベース201を検索して $CID_i$ が登録されていることと $CID_i$ の投票をまだ受付けていないことを確認し(ステップB10-2)、投票データ記録装置204に $(E_i, CID_i)$ と $Se_k$ とを記録するとともに、有権者名簿データベース201に $CID_i$ が投票済みであることを記録する(ステップB11-2)。

#### 【0100】

なお、投票機器100, 110, 140により投票を行なった投票者は、投票データの受け付けが終わった後、投票サーバから受信した公開情報 $(p, q, g, Y)$ と第1の変換データ $(Gr, Yr, r)$ 、第1の変換証明データ $(Gd, d)$ とを変換検証サーバ700の変換証明手段701に入力し、第1の変換データ、第1の変換証明データが正しく公開情報 $(p, q, g, Y)$ から作成されたものかどうかを検証してもよい。また、暗号サーバ400, 410, 440から受信した第2の変換データ $(Gs, Ys, s)$ 、第2の変換証明データ $(Gu, u)$ についても、同様に変換検証サーバ700の変換検証手段701により、公開情報 $(p, q, g, Y)$ から正しく作成されたものかどうかを検証してもよい。

#### 【0101】

投票締切り後の処理については、第1の実施の形態の場合と同じであるので、ここでは説明を省略する。

#### 【0102】

次に、本実施形態の効果について説明する。

#### 【0103】

本実施形態では、投票機器100, 110, 140にそれぞれ暗号データ作成手段104, 114, 144を備え、投票サーバ200に第1の変換手段206を備え、暗号サーバ400, 410, 440にそれぞれ第2の変換手段405, 415, 445を備えることで、投票機器100, 110, 140では複雑な演算を行なうことなく、暗号投票データの作成が行なえる。また、暗号投票データは第1の変換データと第2の変換データの両方をもとに計算されるため、投票サーバ200や暗号サーバ400, 410, 440は、単独では、投票者の暗号投票データから平文の投票内容を知ることはできない。また、暗号データ作成手段104, 114, 144により生成される暗号化証明データは、投票機器120, 130, 150の暗号化手段124, 134, 154が生成する暗号化証明データと同じ処理で検証が可能である。また、投票機器100, 110, 140に暗号データ作成手段104, 114, 144を備えるため、投票内容となる候補者名などあらかじめ決められているような投票に限らず、投票者が自由に投票内容を決める自由記述による投票(やアンケート)などにも本実施形態は適用可能である。

#### 【0104】

また、投票サーバ200が送信する第1の変換データ、第1の変換証明データ、および、暗号サーバ400, 410, 440が送信する第2の変換データ、第2の変換証明データは、変換検証手段701を用いることで、公開情報 $(p, q, g, Y)$ から正しく作成されたものかどうかを確認できる。そのため、投票サーバ200や暗号サーバ400, 410, 440が不正な変換データ、変換証明データを投票機器に送信して投票を妨害しよ

うとした場合、その不正が発覚する。これにより、投票サーバ200、暗号サーバ400、410、440での不正行為を抑止することができる。

#### 【0105】

##### 《第3の実施形態》

次に、本発明の第3の発明形態について図面を参照して説明する。図15に示した第3の実施形態の匿名電子投票システムは、図1に示された第1の実施形態の匿名電子投票システムにおいて、さらに暗号証明検証サーバ600を設けるとともに、投票サーバ200の暗号化手段203に代えて証明付き暗号化手段205を設け、暗号サーバ400、410、440の再暗号化手段401、411、441に代えてそれぞれ証明付き再暗号化手段402、412、442を設け、暗号証明検証サーバ600には暗号化証明検証手段601と再暗号化証明検証手段602とを設けたものである。

#### 【0106】

証明付き暗号化手段205は、暗号化公開鍵Yを含む公開情報と平文データvとを入力とし、Yによりvを暗号化したE(v)と、E(v)がYによりvを正しく暗号化したことを示す証明データwとを出力する。証明付き再暗号化手段402、412、442は、暗号化公開鍵Yを含む公開情報と暗号データE(v)とを入力とし、YによりE(v)を再度暗号化したE'(v)と、E'(v)がYによりE(v)を正しく再度暗号化したことを示す証明データw'とを出力する。

#### 【0107】

暗号化証明検証手段601は、暗号化公開鍵Yを含む公開情報と平文データvと暗号データE(v)と証明データwとを入力とし、E(v)がYによりvを正しく暗号化したものかどうかを検証する。再暗号化証明検証手段602は、暗号化公開鍵Yを含む公開情報と暗号データE(v)とE(v)を再度暗号化したE'(v)と証明データw'とを入力とし、E'(v)がYによりE(v)を正しく暗号化したものかどうかを検証する。

#### 【0108】

特許文献1に示された技術を用いる場合、証明付き暗号化手段205は、公開情報(p, q, g, Y)と平文投票データviを入力とし、暗号投票データE(vi)と証明データwとを出力する。E(vi)は(Gi, Vi)という組で表され、

$$(Gi, Vi) = (g^r \bmod p, vi \times Y^r \bmod p)$$

の計算によって得られる。ここで、rは平文投票データviに対して無作為に選んだ乱数である。そして、証明データwとしてrが出力される。

#### 【0109】

証明付き再暗号化手段205は、公開情報(p, q, g, Y)と暗号投票データE(vi) = (Gi, Vi)とを入力とし、暗号投票データE'(vi)と証明データw'とを出力する。E'(vi)は(G'i, V'i)という組で表され、

$$(G'i, V'i) = (Gi^s \bmod p, Vi \times Y^s \bmod p)$$

の計算によって得られる。ここで、sは平文投票データviに対して無作為に選んだ乱数である。そして、証明データw'としてsが出力される。

#### 【0110】

暗号化証明検証手段601は、viと(p, q, g, Y)とE(vi) = (Gi, Vi)とwとを入力とし、

$$Gi = g^w \bmod p,$$

$$Vi = vi \times Y^w \bmod p$$

の等式が両方とも成り立てば証明を合格と判定し、どちらか一方でも等式が成り立たなければ証明を不正と判定する。

#### 【0111】

再暗号化証明検証手段602は、(Gi, Vi)と(p, q, g, Y)とE'(vi) = (G'i, V'i)とw'とを入力とし、

$$G'i = Gi^{w'} \bmod p,$$

$$V'i = Vi \times Y^{w'} \bmod p$$

の等式が両方とも成り立てば証明を合格と判定とし、どちらか一方でも等式が成り立たなければ証明を不正と判定する。

#### 【0112】

次に、本実施形態の匿名電子投票システムの動作について説明する。図16～図18は、それぞれ、投票機器100、110、140での処理（及びそれらの投票機器での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理）を示しており、図19は、投票受付け後から開票に相当する作業までの処理を説明している。なお、本実施形態での初期設定の動作は第1の実施の形態と同じであり、また、投票機器120、130、150の動作も第1の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

#### 【0113】

以下、投票機器100、110、140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

#### 【0114】

投票機器100、110、140は、投票サーバ200に対し、暗号投票情報要求を送信する。投票サーバ200は、暗号投票情報要求を受信すると、証明付き暗号化手段205により、すべての候補者名 $v_j$ について、 $v_j$ を公開情報 $(p, q, g, Y)$ で暗号化して $E(v_j)$ を作成し、その $E(v_j)$ が $v_j$ を $(p, q, g, Y)$ により正しく暗号化したものであることの証明データ $w_j$ を作成し（図17、図18、図19のステップC6）、公開情報 $(p, q, g, Y)$ と $(v_j, E(v_j), w_j)$ のリストとを投票機器100、110、140に返信する（図16、図17、図18のステップC7）。

#### 【0115】

また、暗号サーバ400、410、440は、投票機器から $E(v_i)$ と公開情報 $(p, q, g, Y)$ とを受信すると、それぞれ証明付き再暗号手段402、412、442に $E(v_i)$ と $(p, q, g, Y)$ を入力し、 $E(v_i)$ を再度暗号化した $E'(v_i)$ と $E(v_i)$ から $(p, q, g, Y)$ により正しく暗号化したことの証明データ $w'_i$ とを作成し（図16、図17、図18のステップC100-1、C110-1、C140-1）、投票機器100、110、140に $E'(v_i)$ と $w'_i$ とを返信する（図16、図17、図18のステップC100-2、C110-2、C140-2）。

#### 【0116】

以上が投票データの送信までの処理のうち、第1の実施形態と異なる部分である。

#### 【0117】

次に、図19のフローチャートを参照し、投票受付け後の投票者の処理について説明する。

#### 【0118】

投票機器100、110、140により投票を行なった投票者は、投票データの受付けが終わった後、投票サーバ200から受信した公開情報 $(p, q, g, Y)$ と $(v_j, E(v_j), w_j)$ のリストと、暗号サーバから受信した $(E'(v_i), w'_i)$ と $E(v_i)$ とを暗号証明検証サーバ600に送信する（ステップC15）。暗号証明検証サーバ600は、公開情報 $(p, q, g, Y)$ と $(v_j, E(v_j), w_j)$ のリストとを暗号化証明検証手段601に入力し、すべての $E(v_j)$ が $v_j$ を $(p, q, g, Y)$ により正しく暗号化されているかどうかを検証し（ステップC16）、さらに、 $(E'(v_i), E(v_i), w')$ を再暗号化検証手段602に入力し、 $E'(v_i)$ が $E(v_i)$ を $(p, q, g, Y)$ により正しく再度暗号化したものかどうかを検証し（ステップC17）、検証結果を出力する（ステップC18）。

#### 【0119】

次に、本実施形態の効果について説明する。

#### 【0120】

本実施形態では、投票サーバ200に証明付き暗号化手段205を備え、投票機器には $(v_j, E(v_j), w_j)$ のリストが送信され、暗号化証明検証手段601により $E$

$v_j$ ) が  $v_j$  を  $(p, q, g, Y)$  により正しく暗号化されたものかどうかを確認できるため、投票サーバ200が  $v_j$  を暗号化したものと偽って  $(v_j, E(v'_j), w)$  を投票機器に送信した場合、その不正が発覚する。これにより、投票サーバ200での不正行為を抑止することができる。

#### 【0121】

また、暗号サーバ400、410、440にそれぞれ証明付き再暗号手段402、412、442を備え、投票機器には  $E'(v_i)$ 、 $E(v_i)$ 、 $w'$  が送信され、暗号化証明検証手段602により  $E'(v_i)$  が  $E(v_i)$  を  $(p, q, g, Y)$  により正しく暗号化したものかどうかを確認できるため、暗号サーバが  $E(v_i)$  を再度暗号化したものと偽って  $E'(v)$ 、 $E(v_i)$ 、 $w'$  を投票機器に返信した場合、その不正が発覚する。これにより、暗号サーバ400、410、440での不正行為を抑止することができる。

#### 【0122】

なおここでは、暗号化証明検証手段601を別のサーバ(暗号証明検証サーバ600)に備え、投票終了後に検証を行なう構成を示したが、投票機器内にその構成要素として暗号化証明検証手段を設け、投票中に検証を行なえるようにする構成も可能である。また、暗号化検証手段を構成要素として暗号サーバ内に設け、投票サーバの暗号証明の検証のみを投票中に行ない、暗号サーバの証明データの検証のみを投票後に行なう構成をとることも可能である。また、投票機器に暗号化証明検証手段601と再暗号化証明検証手段602とを備え、投票中にすべての検証を行なう構成にしてもよい。

#### 【0123】

##### 《第4の実施形態》

次に、本発明の第4の実施形態について図面を参照して説明する。第1の実施形態の匿名電子投票システムにおいて、1つの投票機器が複数の暗号サーバを用いるようにすることによって、投票の秘密をさらに頑強(ロバスト)に守ることができるようになる。本実施形態は、1つの投票機器に対応する暗号サーバの台数を増やしたものである。

#### 【0124】

図20に示した第4の実施形態の匿名電子投票システムは、図1に示された第1の実施形態の匿名投票システムにおいて、 $k$  を2以上の整数として、投票機器100が  $k$  台の暗号サーバ400-1~400- $k$ と接続し、同様に投票機器110、140がそれぞれ暗号サーバ410-1~410- $k$ 、暗号サーバ440-1~440- $k$ と接続されるようにしたものである。各暗号サーバ400-1~400- $k$ 、410-1~410- $k$ 、440-1~440- $k$ には、それぞれ、再暗号化手段401-1~401- $k$ 、411-1~411- $k$ 、441-1~441- $k$ が備えられている。投票機器100、110、120、130、140、150、投票サーバ200及び認証サーバ300の構成は、図1に示した第1の実施形態の場合と同じである。

#### 【0125】

次に、本実施形態の匿名電子投票システムの動作について説明する。図21~図23は、それぞれ、投票機器100、110、140での処理(及びそれらの投票機器での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理)を示している。なお、本実施形態での初期設定の動作は第1の実施の形態と同じであり、また、投票機器120、130、150の動作も第1の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

#### 【0126】

以下、投票機器100、110、140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

#### 【0127】

投票機器100、110、140は、投票サーバ200へ暗号投票情報要求を送信する(図21、図22、図23のステップA5-1)。投票サーバ200は、暗号投票情報要求を受信すると、その暗号化手段203により、すべての候補者名  $v_j$  について、 $v_j$  を

公開情報 (p, q, g, Y) で暗号化して  $E(v_j)$  を作成し (図21、図22、図23のステップA6)、公開情報 (p, q, g, Y) と  $(v_j, E(v_j))$  のリストとを投票機器100, 110, 140に返信する (図21、図22、図23のステップA7-1)。投票機器100, 110, 140は、(p, q, g, Y) と  $(v_j, E(v_j))$  のリストとを受信すると、その表示装置101, 111, 141において  $v_j$  のリストを投票者に表示し、投票者は入力装置102, 112, 142により  $v_j$  のリストから候補者  $v_i$  を選択して入力する (図21、図22、図23のステップA100-1、A110-1、A140-1)。

#### 【0128】

そして、投票機器100, 110, 140は、 $v_i$  に対応する暗号データ  $E(v_i)$  と公開情報 (p, q, g, Y) とを1番目の暗号サーバ400-1, 410-1, 440-1に送信する (図21、図22、図23のステップD101-1, D111-1, D141-1)。暗号サーバ400-1, 410-1, 440-1は、受信した暗号データ  $E(v_i)$  と公開情報 (p, q, g, Y) とを再暗号化手段401-1, 410-1, 440-1に入力して  $E(v_i)$  を再度暗号化した  $E'(v_i)$  を計算し (図21、図22、図23のステップD101-2, D111-2, D141-2)、 $E'(v_i)$  を投票機器100, 110, 140に返信する (図21、図22、図23のステップD101-3, D111-3, D141-3)。次に、投票機器100, 110, 140は、1番目の暗号サーバ400-1, 410-1, 440-1から得た  $E'(v_i)$  を2番目の暗号サーバ400-2, 410-2, 440-2に対して送信することにより、 $E'(v_i)$  をもう一回暗号化させて  $E'(v_i)$  を得る。以下、このような処理を  $k$  個の暗号サーバ400-1~400- $k$ , 410-1~410- $k$ , 440-1~440- $k$  のすべてについて繰り返し、暗号データ  $E'(v_i)$  を得る (図21、図22、図23のステップD10 $k$ -3, D11 $k$ -3, D14 $k$ -3)。暗号データ  $E'(v_i)$  は  $E(v_i)$  を  $k$  回にわたって再暗号化したデータに該当する。投票機器100, 110, 140は、 $E'(v_i)$  を認証サーバ300や投票サーバ200へ送る暗号データ  $E'(v_i)$  とする (図21、図22、図23のステップD100-6, D110-5, D140-5)。以降の処理は、第1の実施形態における処理と同じである。

#### 【0129】

次に、本実施形態の効果について説明する。

#### 【0130】

本実施形態では、投票機器100, 110, 140に、それぞれ、暗号サーバ400-1~400- $k$ 、暗号サーバ410-1~410- $k$ 、暗号サーバ440-1~440- $k$ が接続され、投票機器100, 110, 140は、投票サーバ200から受信した暗号データ  $E(v_i)$  を合計  $k$  回にわたって再暗号化して得られる  $E'(v_i)$  を投票サーバ200に送る。そのため、投票サーバと  $k$  個の暗号サーバとがすべて結託しない限り、 $E'(v_i)$  から平文の投票内容  $v_i$  が判明することはなく、投票の秘密をより強く求めることができる。

#### 【0131】

なお、ここでは、投票機器100, 110, 140に接続される暗号サーバの個数をいづれも  $k$  個としたが、同数である必要はなく、それぞれ別の数であってもよい。また、第1の実施形態と同じく、いくつかの投票機器がいくつかの暗号サーバを共用することも可能である。

#### 【0132】

また、図15に示された第3の実施形態の場合と同様に、各暗号サーバには証明付き再暗号化手段を備え、暗号化の証明データを作成するようにしてもよい。

#### 【0133】

#### 《第5の実施形態》

次に、本発明の第5の実施形態について図面を参照して説明する。第2の実施形態の匿名電子投票システムにおいて、1つの投票機器が複数の暗号サーバを用いるようにするこ

とによって、投票の秘密をさらに頑強（ロバスト）に守ることができるようになる。本実施形態は、1つの投票機器に対応する暗号サーバの台数を増やしたものである。

#### 【0134】

図24に示した第5の実施形態の匿名電子投票システムは、図10に示された第2の実施形態の匿名投票システムにおいて、 $k$ を2以上の整数として、投票機器100が $k$ 台の暗号サーバ400-1~400- $k$ と接続し、同様に投票機器110, 140がそれぞれ暗号サーバ410-1~410- $k$ 、暗号サーバ440-1~440- $k$ と接続されるようにしたものである。各暗号サーバ400-1~400- $k$ , 410-1~410- $k$ , 440-1~440- $k$ には、それぞれ、第2の変換手段405-1~405- $k$ , 415-1~415- $k$ , 445-1~445- $k$ が備えられている。 $m$ は $1 \leq m \leq k$ である整数として、 $m$ 番目の暗号サーバ400- $m$ , 410- $m$ , 440- $m$ の第2の変換手段405- $m$ , 415- $m$ , 445- $m$ は、第2の変換データ( $G_{sm}$ ,  $Y_{sm}$ ,  $s_m$ )と第2の変換証明データ( $G_{um}$ ,  $u_m$ )を作成する。ここで、

$$(G_{sm}, Y_{sm}, s_m) = (g^{sm} \bmod p, Y^{sm} \bmod p, s_m)$$

,  
 $(G_{um}, u_m) = (g^{um} \bmod p, u_m)$   
 である。

#### 【0135】

投票機器100, 110, 140の暗号データ作成手段104, 114, 144は、投票サーバからの第1の変換データ( $G_r$ ,  $Y_r$ ,  $r$ ) = ( $g^r \bmod p$ ,  $Y^r \bmod p$ ,  $r$ )及び第1の変換証明データ( $G_d$ ,  $d$ ) = ( $g^r \bmod p$ ,  $d$ )と、 $k$ 個の暗号サーバからの $k$ 個の第2の変換データ( $G_{s1}$ ,  $Y_{s1}$ ,  $s_1$ ) ~ ( $G_{sk}$ ,  $Y_{sk}$ ,  $s_k$ )及び $k$ 個の第2の変換証明データ( $G_{u1}$ ,  $u_1$ ) ~ ( $G_{uk}$ ,  $u_k$ )と、平文の投票内容 $v_i$ とを入力されると、下記式にしたがって、暗号投票データ $E(v_i)$ を計算する。

#### 【0136】

$$E(v_i) = (G_i, V_i) \\ = (G_r \times G_{s1} \times G_{s2} \times \dots \times G_{sk} \bmod p, v_i \times Y_r \times Y_{s1} \times Y_{s2} \times \dots \times Y_{sk} \bmod p)$$

さらに、暗号データ作成手段104, 114, 144は、  
 $a = G_u \times G_{d1} \times G_{d2} \times \dots \times G_{dk} \bmod p$ ,  
 $c = \text{HASH}(p, q, g, Y, G_i, V_i, a)$ ,  
 $t = c \times (r + s_1 + s_2 + \dots + s_k) + u + d_1 + d_2 + \dots + d_k \bmod q$   
 を計算して、暗号化証明データ( $a$ ,  $t$ )を計算し、暗号投票データ( $G_i$ ,  $V_i$ )とともに出力する。

#### 【0137】

この証明は、暗号化証明検証手段207により、  
 $c = \text{HASH}(p, q, g, Y, G_i, V_i, a)$   
 を計算して、  
 $g^t \times G_i^{-c} = a \bmod p$   
 が成り立つかどうかを確認することで、検証できる。

#### 【0138】

なお、投票機器120, 130, 150、投票サーバ200及び認証サーバ300の構成は、図10に示した第2の実施形態の場合と同じである。

#### 【0139】

次に、本実施形態の匿名電子投票システムの動作について説明する。図25~図27は、それぞれ、投票機器100, 110, 140での処理（及びそれらの投票機器での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理）を示している。なお、本実施形態での初期設定の動作は第2の実施の形態と同じであり、また、投票機器120, 130, 150の動作も第2の実施の形態におけるものと同じであるから、これらの動作に

ついては記載を省略する。

#### 【0140】

以下、投票機器100, 110, 140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

#### 【0141】

投票機器100, 110, 140は、投票サーバ200への変換データ要求を送信する(図25、図26、図27のステップB5)。投票サーバ200は、変換データ要求を受信すると、第1の変換手段206に公開情報(p, q, g, Y)を入力し、第1の変換データ( $G_r$ ,  $Y_r$ , r)と第1の変換証明データ( $G_d$ , d)とを作成し(図25、図26、図27のステップB6)、投票機器100, 110, 140に、(p, q, g, Y), ( $G_r$ ,  $Y_r$ , r), ( $G_d$ , d)を返信する(図25、図26、図27のステップB7)。投票機器100, 110, 140は、投票サーバ200から(p, q, g, Y), ( $G_r$ ,  $Y_r$ , r), ( $G_d$ , d)を受信すると、それぞれ、暗号サーバ400-1, 410-1, 440-1に(p, q, g, Y)と変換データ要求とを送信する(図25、図26、図27のステップE101-1, E111-1, E141-1)。暗号サーバ400-1, 410-1, 440-1は、公開情報(p, q, g, Y)と変換データ要求とを受信すると、それぞれ、第2の変換手段405-1, 415-1, 445-1に(p, q, g, Y)を入力して、第2の変換データ( $G_{s1}$ ,  $Y_{s1}$ , s1)と第2の変換証明データ( $G_{u1}$ , u1)とを生成し(図25、図26、図27のステップE101-2, E111-2, E141-2)、投票機器100, 110, 140に、( $G_{s1}$ ,  $Y_{s1}$ , s1)と( $G_{u1}$ , u1)とを返信する(図25、図26、図27のステップE101-3, E111-3, E141-3)。次に、投票機器100, 110, 140は、2番目の暗号サーバ400-1, 410-1, 440-1に対して同じ処理を繰り返し、以下同様にして、k個の暗号サーバ400-1~400-k, 410-1~410-k, 440-1~440-kのすべてについて繰り返し、k個の第2の変換データ( $G_{s1}$ ,  $Y_{s1}$ , s1)~( $G_{sk}$ ,  $Y_{sk}$ , s<sub>k</sub>)とk個の第2の変換証明データ( $G_{u1}$ , u1)~( $G_{uk}$ , u<sub>k</sub>)とを得る(図25、図26、図27のステップE10k-3, E11k-3, E14k-3まで)。

#### 【0142】

続いて投票機器100, 110, 140は、投票者が入力したv<sub>i</sub>と、第1の変換データ( $G_r$ ,  $Y_r$ , r)、第1の変換証明データ( $G_d$ , d)、k個の第2の変換データ( $G_{s1}$ ,  $Y_{s1}$ , s1)~( $G_{sk}$ ,  $Y_{sk}$ , s<sub>k</sub>)及びk個の第2の変換証明データ( $G_{u1}$ , u1)~( $G_{uk}$ , u<sub>k</sub>)とを暗号データ作成手段104, 114, 144に入力し、暗号投票データE(v<sub>i</sub>)と暗号化証明データ(a, t)とを計算する(図25、図26、図27のステップE100-4, E110-4, E140-4)。これ以降の処理は、第2の実施形態の場合と同様である。

#### 【0143】

次に、本実施形態の効果について説明する。

#### 【0144】

本実施形態では、投票機器100, 110, 140に、それぞれ、暗号サーバ400-1~400-k、暗号サーバ410-1~410-k、暗号サーバ440-1~440-kが接続され、投票機器100, 110, 140は、投票サーバ200から受信した第1の変換データとk個の暗号サーバから受信したk個の第2の変換データにより暗号データE(v<sub>i</sub>)を作成し、この暗号データE(v<sub>i</sub>)を投票サーバ200に送る。そのため、投票サーバとk個の暗号サーバがすべて結託しない限り、E'(v<sub>i</sub>)から平文の投票内容v<sub>i</sub>が判明することはない、投票の秘密をより強く求めることができる。

#### 【0145】

なお、ここでは、投票機器100, 110, 140に接続される暗号サーバの個数をいづれもk個としたが、同数である必要はなく、それぞれ別の数であってもよい。また、第2の実施形態と同じく、いくつかの投票機器がいくつかの暗号サーバを共用することも可

能である。

#### 【0146】

なお、投票サーバ200に第1の変換手段を備えない構成とし、k個の暗号サーバから受信した第2の変換データ、第2の変換証明データのみを用いて暗号投票データE(vi)及び暗号化証明データ(α, t)を作成することとしてもよい。この場合、投票機器100, 110, 140を含めすべての投票機器は投票サーバ200に単なる投票情報要求を送信し、投票サーバ200はすべての投票機器に対して公開情報(p, q, g, Y)と候補者情報を送信する。投票機器100, 110, 140の暗号データ作成手段104, 114, 144は、k個の第2の変換データ(Gs1, Ys1, s1)～(Gsk, Ysk, sk)及びk個の第2の変換証明データ(Gd1, d1)～(Gdk, dk)により、下記のように暗号投票データE(vi)、暗号化証明データ(α, t)を計算する。

#### 【0147】

$$\begin{aligned} E(vi) &= (Gi, Vi) \\ &= (Gs1 \times Gs2 \times \dots \times Gsk \bmod p, vi \times Ys1 \times Ys2 \times \dots \times Ysk \bmod p), \\ \alpha &= Gd1 \times Gd2 \times \dots \times Gdk \bmod p, \\ c &= \text{HASH}(p, q, g, Y, Gi, Vi, \alpha), \\ t &= c \times (s1 + s2 + \dots + sk) + d1 + d2 + \dots + dk \bmod q \end{aligned}$$

#### 【0148】

なお、投票サーバは、第1の変換データ、第1の変換証明データをあらかじめ計算しておくことも可能であるし、同様に、公開情報(p, q, g, Y)をあらかじめ暗号サーバに配布しておき、第2の変換データ、第2の変換証明データを事前に計算しておくようにすることも可能である。

#### 【0149】

以上、本発明の好ましい実施の形態について説明したが、上述した匿名電子投票システムを構成する投票機器、投票サーバ、認証サーバ、暗号サーバ及び暗号証明検証サーバは、いずれも、それらの機能を実現するためのコンピュータプログラムを、サーバ用コンピュータやパーソナルコンピュータなどのコンピュータに読み込ませ、そのプログラムを実行させることによっても実現できる。こうしたコンピュータプログラムは、磁気テープやCD-ROMなどの記録媒体によって、あるいは、ネットワークを介してコンピュータに読み込まれる。言い換えれば、投票機器、投票サーバ、認証サーバ、暗号サーバ及び暗号証明検証サーバにおけるそれぞれの構成要素は、いずれも、ソフトウェアによってもハードウェアによっても実現できるものである。

#### 【0150】

特に、投票機器を実現するためのコンピュータとしては、データ処理能力とネットワーク接続機能とを有する携帯電話機や各種の携帯情報端末(PDA)などの、コンピュータとして見たときには比較的处理能力や記憶能力が小さいものを使用することができる。

#### 【産業上の利用可能性】

#### 【0151】

本発明は、ネットワークなどを介した匿名電子投票システムという用途に適用できる。また、投票内容として自由記述を許すことにより、ネットワークなどを介した匿名電子アンケートシステムという用途に適用できる。

#### 【図面の簡単な説明】

#### 【0152】

【図1】 本発明の第1の発明形態の匿名電子投票システムの構成を示すブロック図である。

【図2】 第1の実施形態における初期設定の動作を示すフローチャートである。

【図3】 第1の実施形態における投票機器100の動作を示すフローチャートである。

【図4】 第1の実施形態における投票機器110の動作を示すフローチャートである。

- 。【図 5】第 1 の実施形態における投票機器 120 の動作を示すフローチャートである。
- 。【図 6】第 1 の実施形態における投票機器 130 の動作を示すフローチャートである。
- 。【図 7】第 1 の実施形態における投票機器 140 の動作を示すフローチャートである。
- 。【図 8】第 1 の実施形態における投票機器 150 の動作を示すフローチャートである。
- 。【図 9】第 1 の実施形態における投票サーバ 200 の動作を示すフローチャートである。
- 【図 10】本発明の第 2 の実施形態の匿名電子投票システムの構成を示すブロック図である。
- 【図 11】第 2 の実施形態における投票機器 100 の動作を示すフローチャートである。
- 【図 12】第 2 の実施形態における投票機器 110 の動作を示すフローチャートである。
- 【図 13】第 2 の実施形態における投票機器 140 の動作を示すフローチャートである。
- 【図 14】第 2 の実施形態における投票サーバ 200 の動作を示すフローチャートである。
- 【図 15】本発明の第 3 の実施形態の匿名電子投票システムの構成を示すブロック図である。
- 【図 16】第 3 の実施形態における投票機器 100 の動作を示すフローチャートである。
- 【図 17】第 3 の実施形態における投票機器 110 の動作を示すフローチャートである。
- 【図 18】第 3 の実施形態における投票機器 140 の動作を示すフローチャートである。
- 【図 19】第 3 の実施形態における暗号検証サーバ 600 の動作を示すフローチャートである。
- 【図 20】本発明の第 4 の実施形態の構成を示すブロック図である。
- 【図 21】第 4 の実施形態における投票機器 100 の動作を示すフローチャートである。
- 【図 22】第 4 の実施形態における投票機器 110 の動作を示すフローチャートである。
- 【図 23】第 4 の実施形態における投票機器 140 の動作を示すフローチャートである。
- 【図 24】本発明の第 5 の実施形態の構成を示すブロック図である。
- 【図 25】第 5 の実施形態における投票機器 100 の動作を示すフローチャートである。
- 【図 26】第 5 の実施形態における投票機器 110 の動作を示すフローチャートである。
- 【図 27】第 5 の実施形態における投票機器 140 の動作を示すフローチャートである。
- 【図 28】従来の匿名電子投票システムの構成を示すブロック図である。

## 【符号の説明】

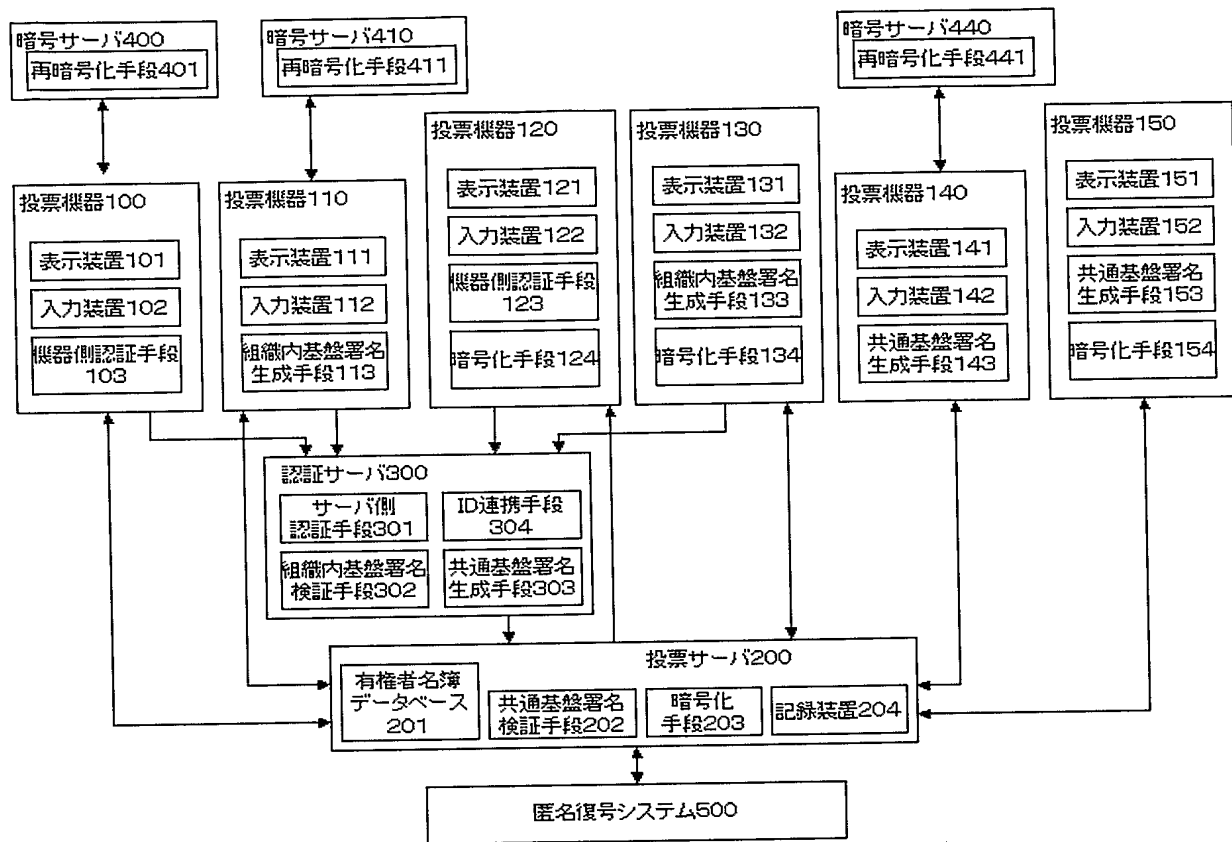
【0153】

100, 110, 120, 130, 140, 150	投票機器
101, 111, 121, 131, 141, 151	入力装置

102, 112, 122, 132, 142, 152 表示装置  
103, 123 機器側認証手段  
104, 114, 144 暗号データ作成手段  
113, 133 組織内基盤署名生成手段  
143, 153, 303 共通基盤署名生成手段  
134, 154, 203 暗号化手段  
200 投票サーバ  
201 有権者名簿データベース  
202 共通基盤署名検証手段  
204 記録装置  
205 証明付き暗号化手段  
206 第1の変換手段  
207 暗号化証明検証手段  
300 認証サーバ  
301 サーバ側認証手段  
302 組織内署名検証手段  
304 ID連携手段  
400, 400-1~400-k, 410, 410-1~410-k, 440, 440-1~440-k 暗号サーバ  
401, 401-1~401-k, 411, 411-1~411-k, 441, 441-1~441-k 再暗号化手段  
402, 412, 442 証明付き再暗号化手段  
405, 405-1~405-k, 415, 415-1~415-k, 445, 445-1~445-k 第2の変換手段  
500 匿名復号システム  
600 暗号証明検証サーバ  
601 暗号化証明検証手段  
602 再暗号化証明検証手段  
700 変換検証サーバ  
701 変換検証手段

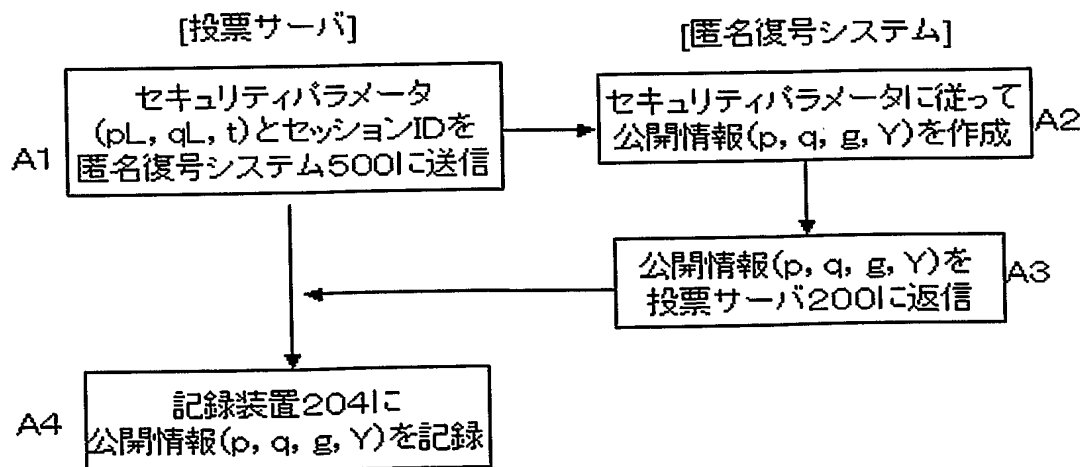
【書類名】 図面

【図 1】

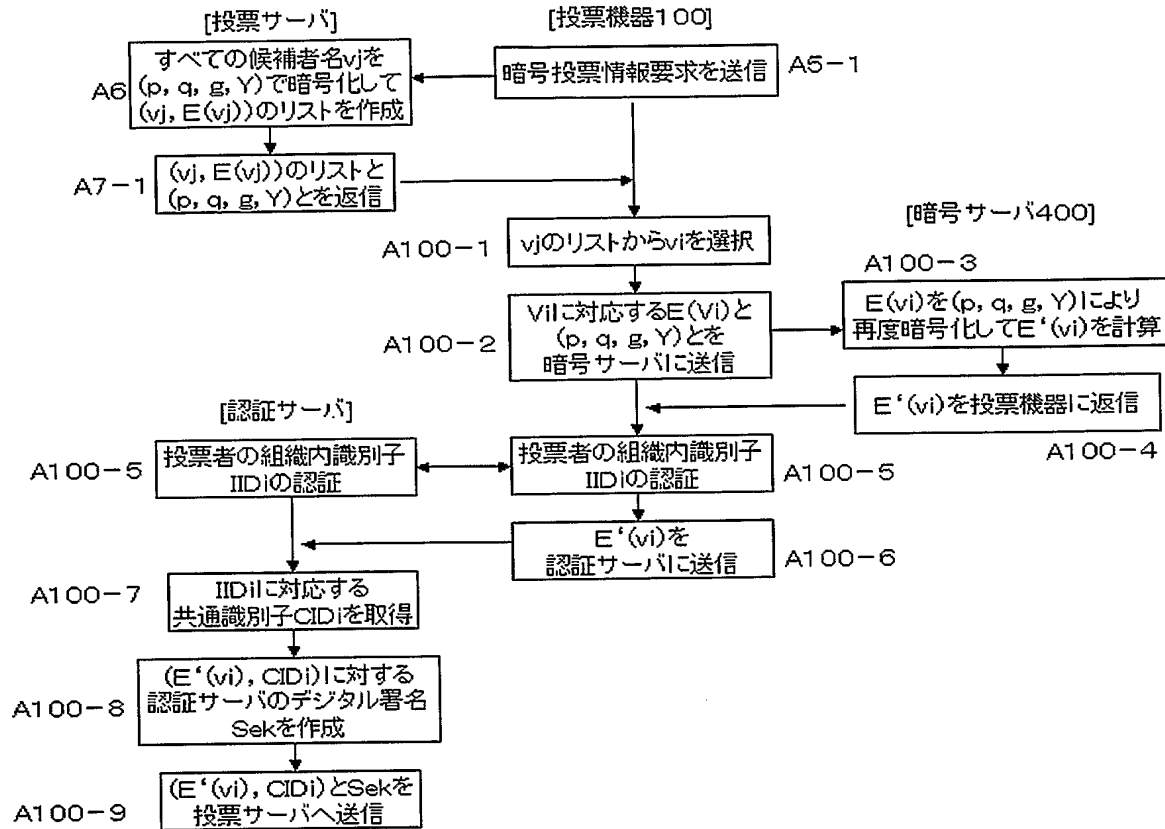


【図 2】

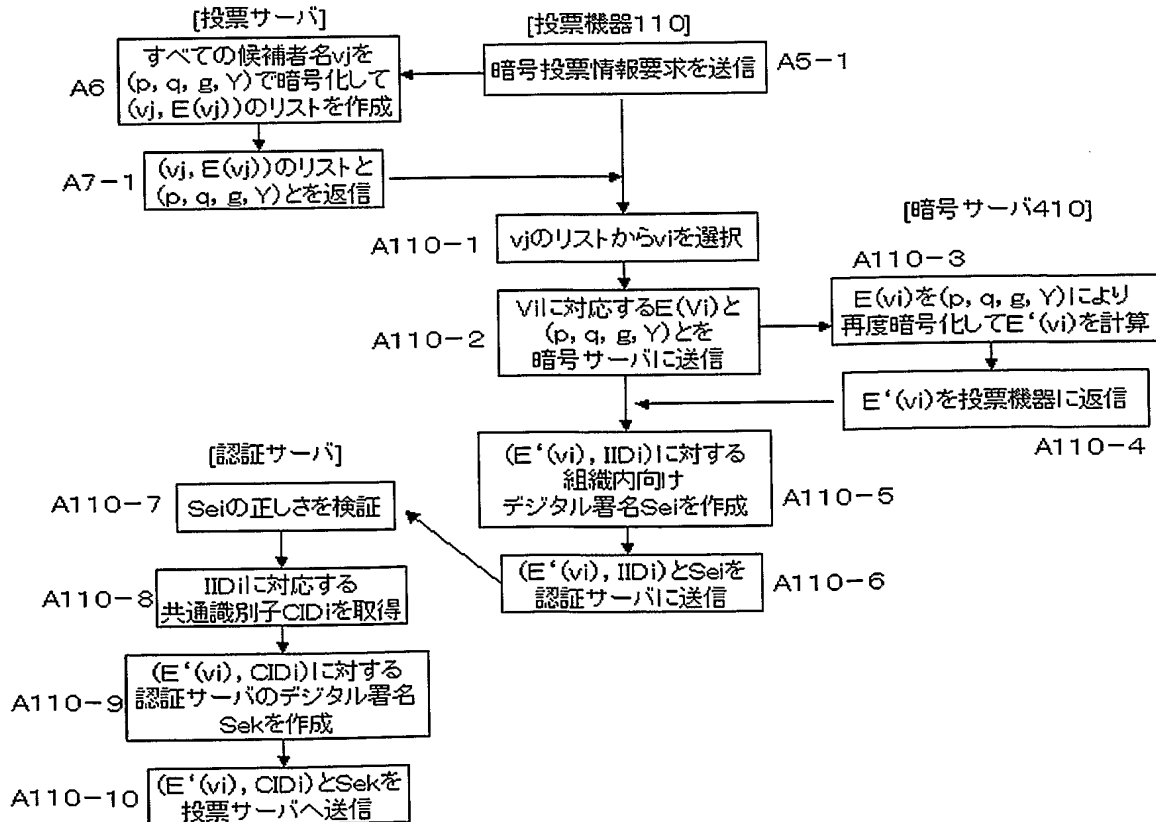
(初期設定)



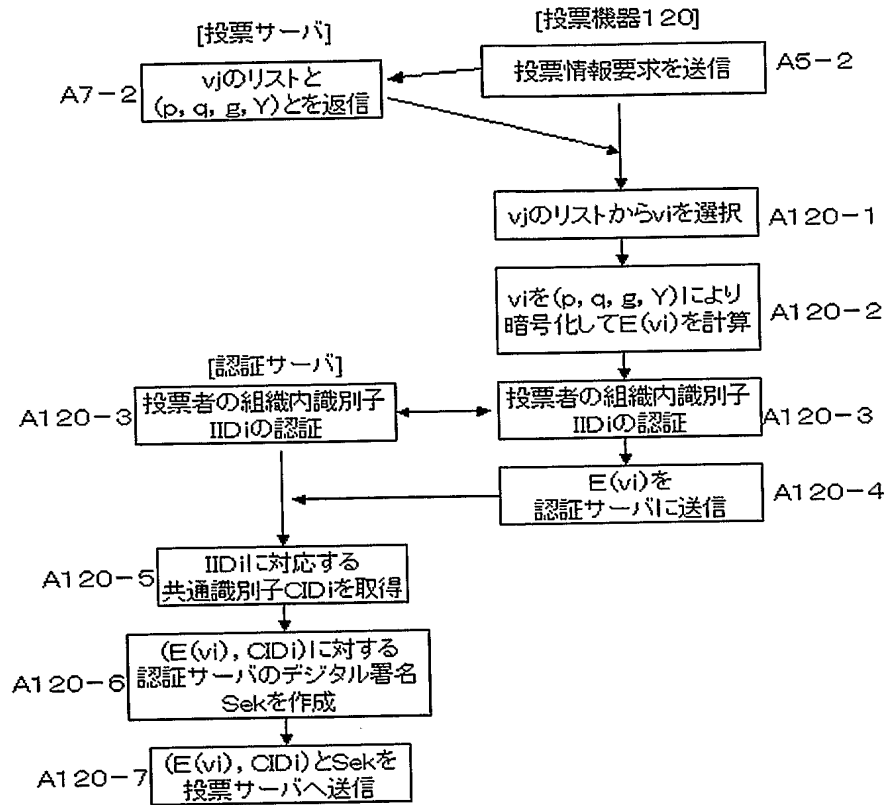
【図 3】



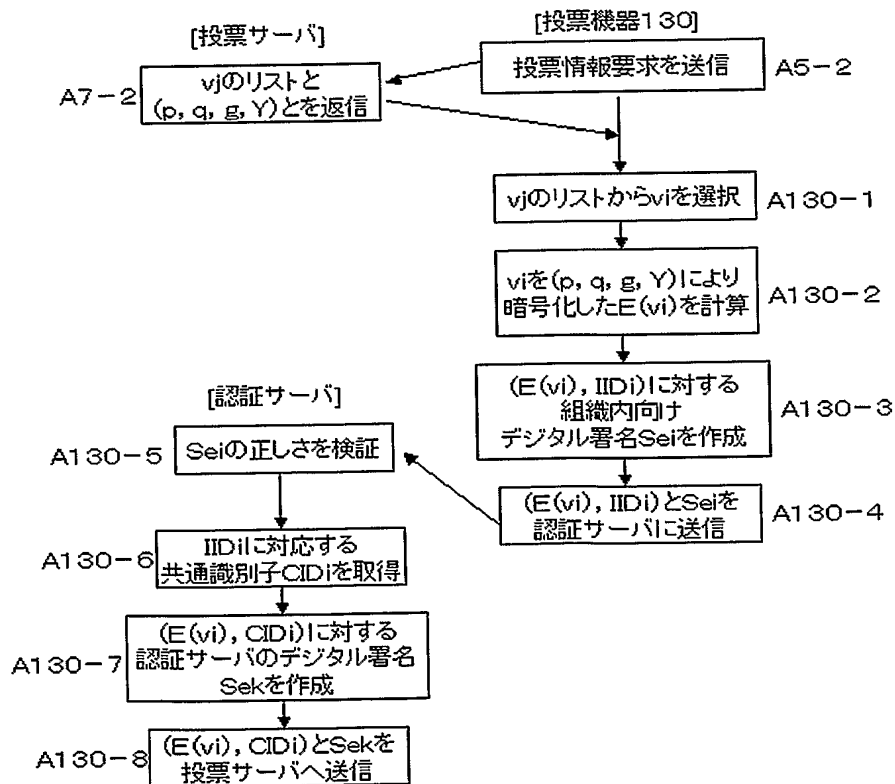
【図 4】



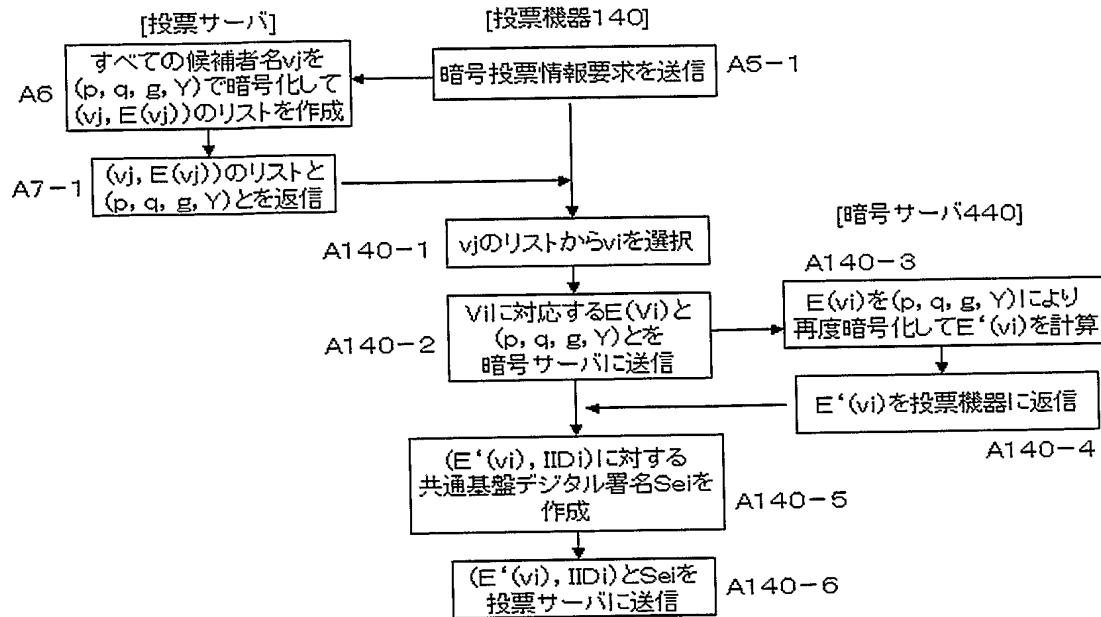
【図 5】



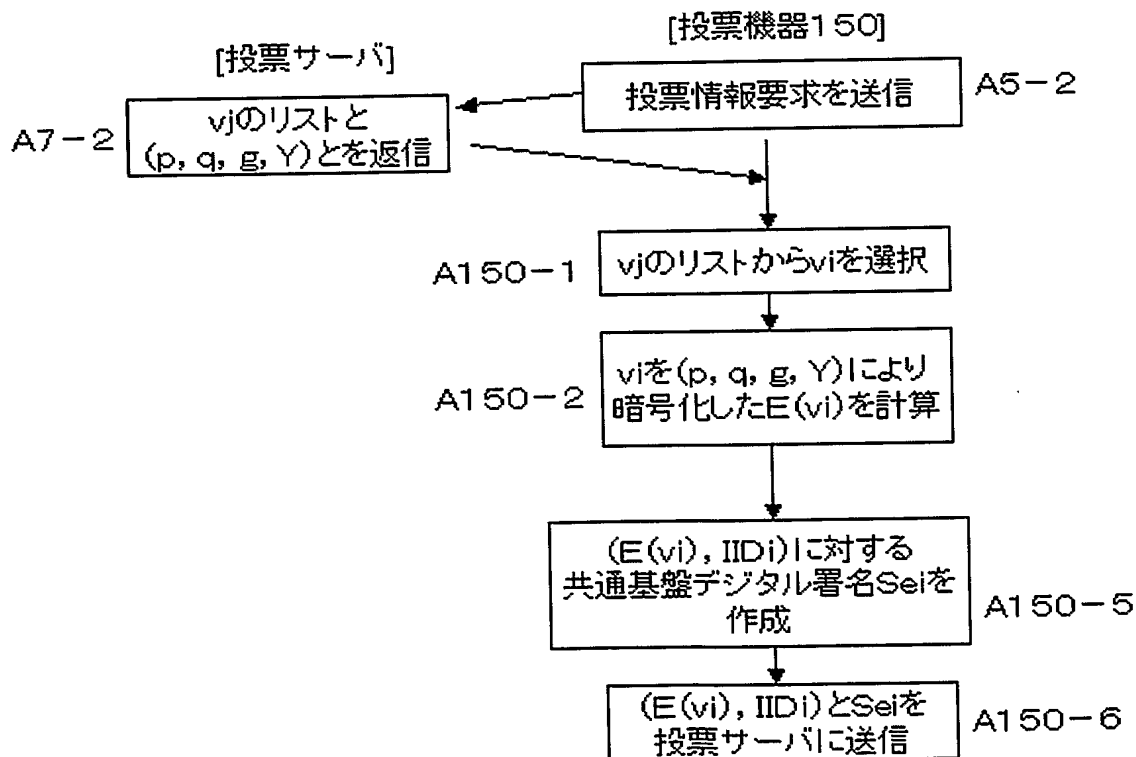
【図 6】



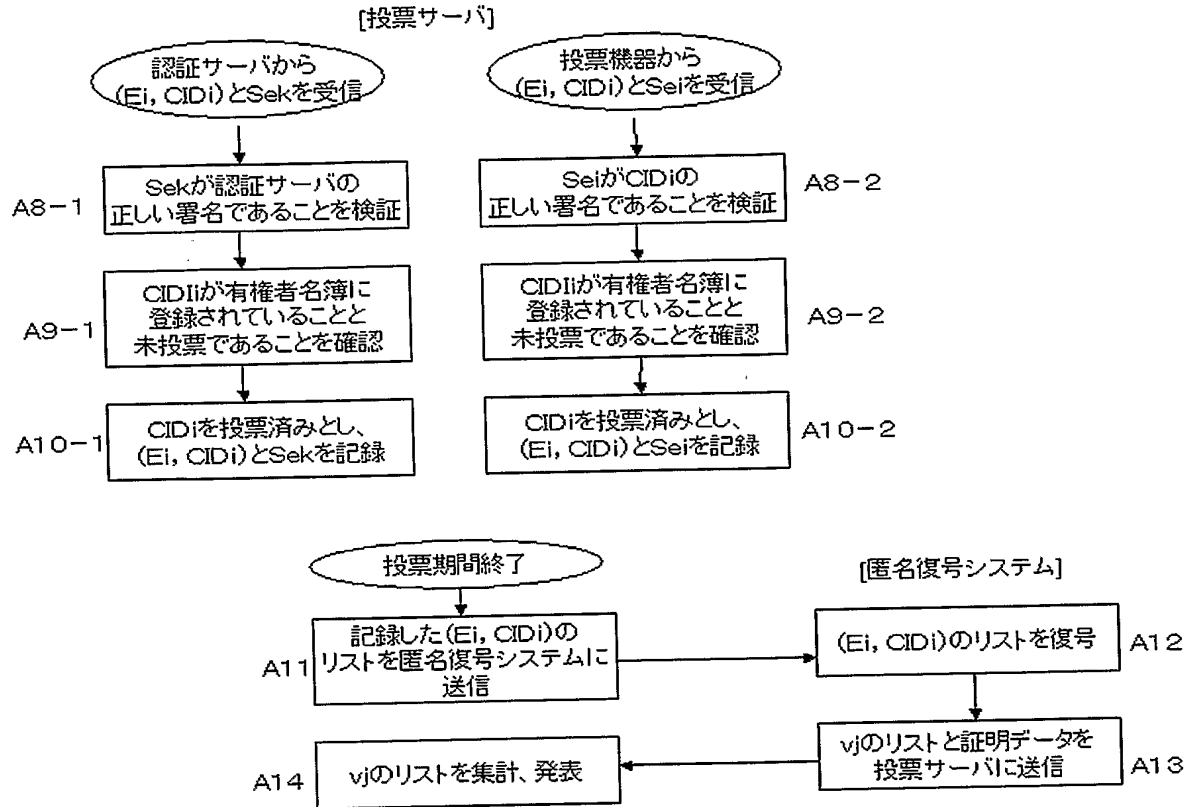
【図 7】



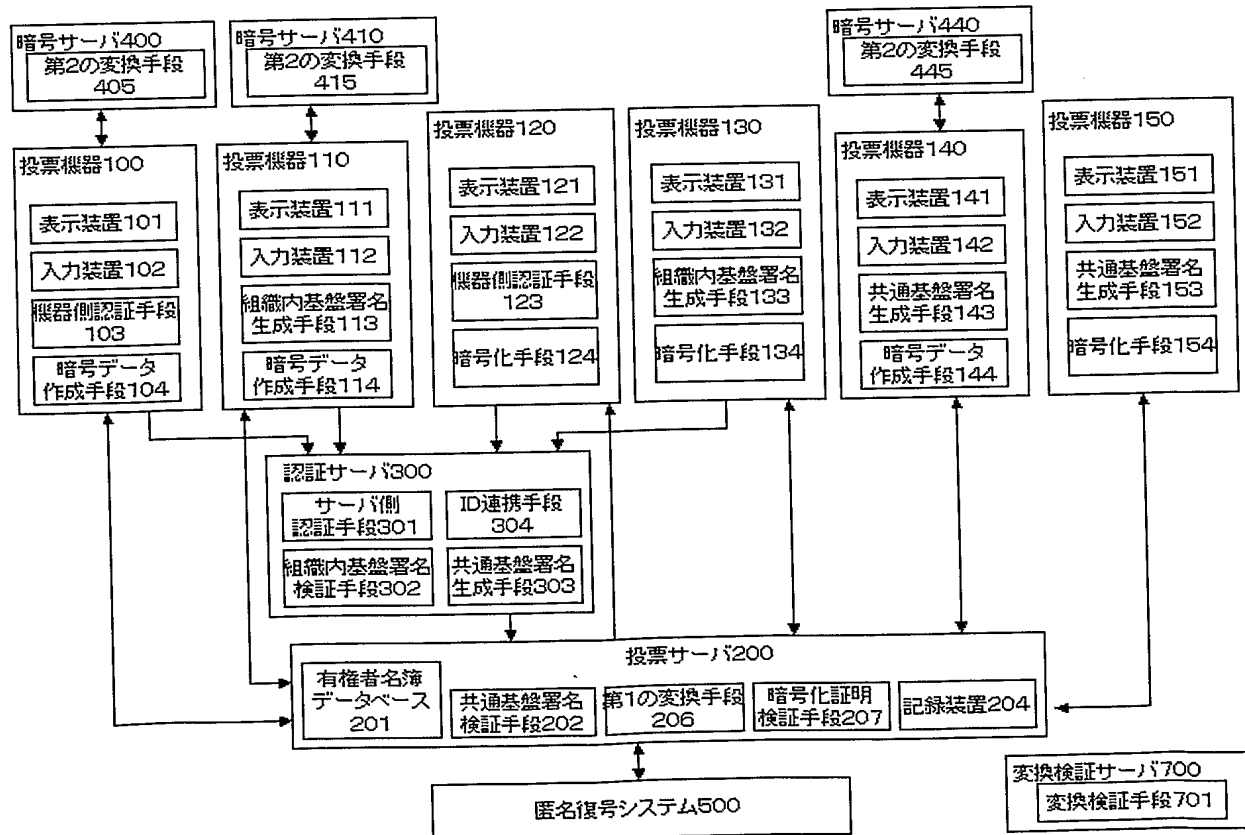
【図 8】



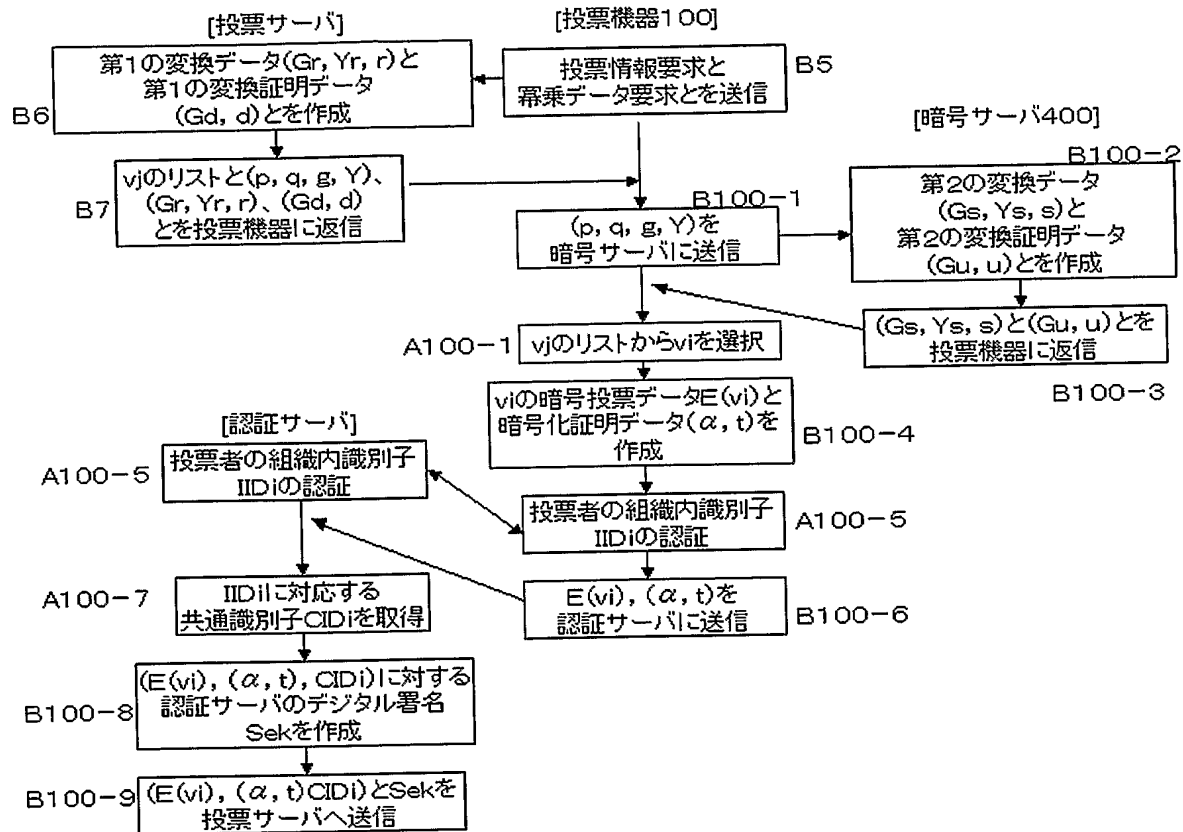
【図 9】



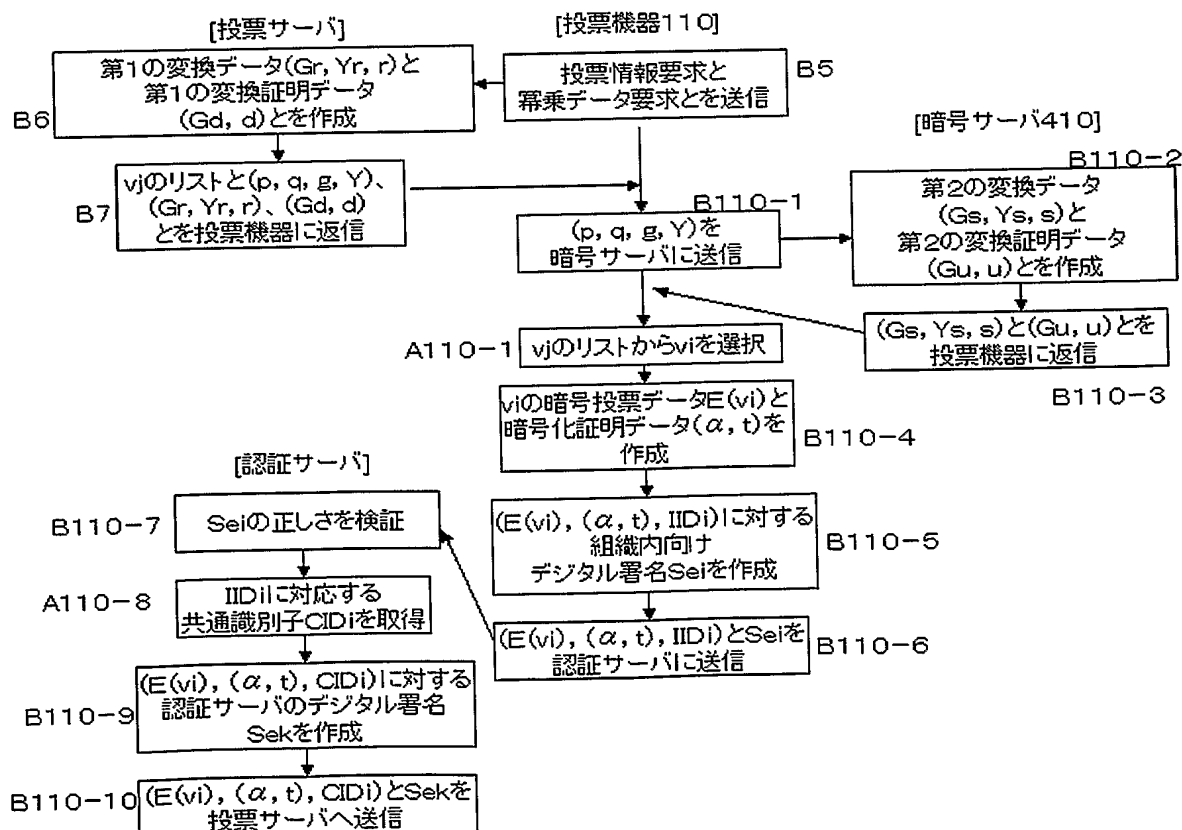
【図 10】



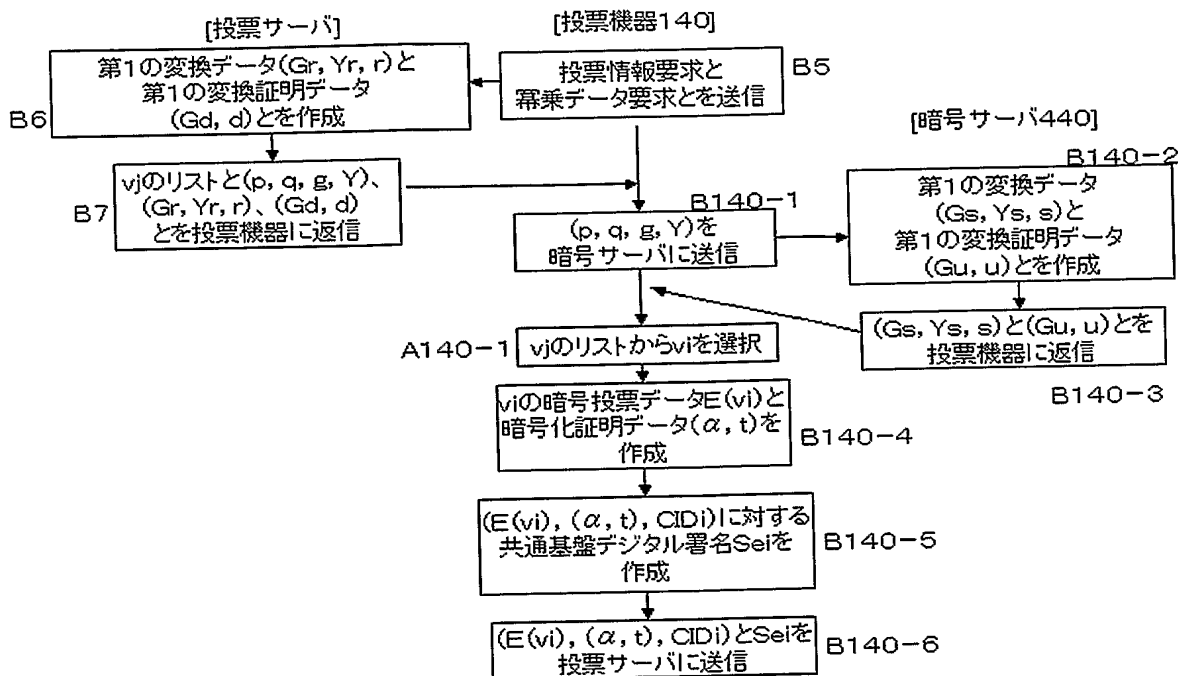
【図 11】



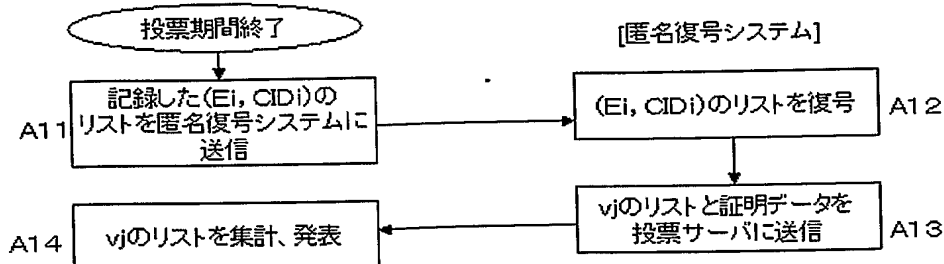
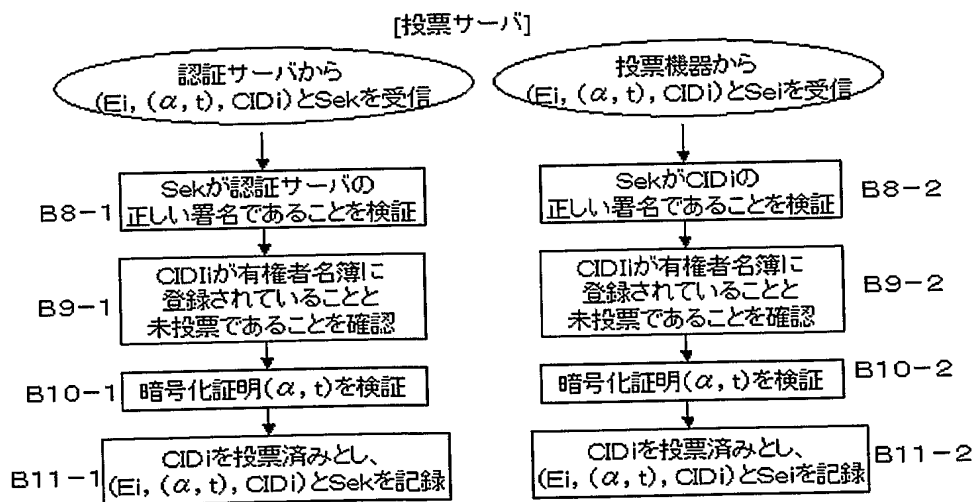
【図 12】



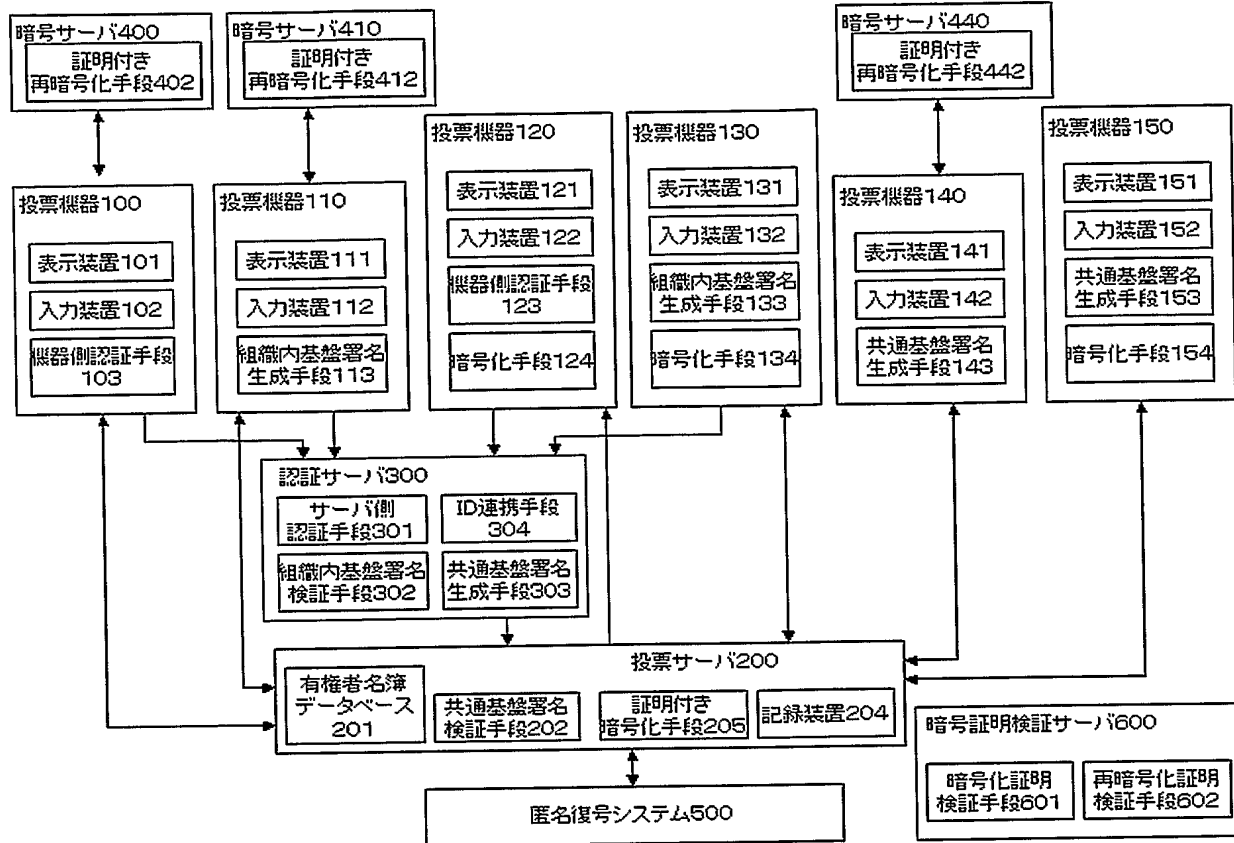
【図 13】



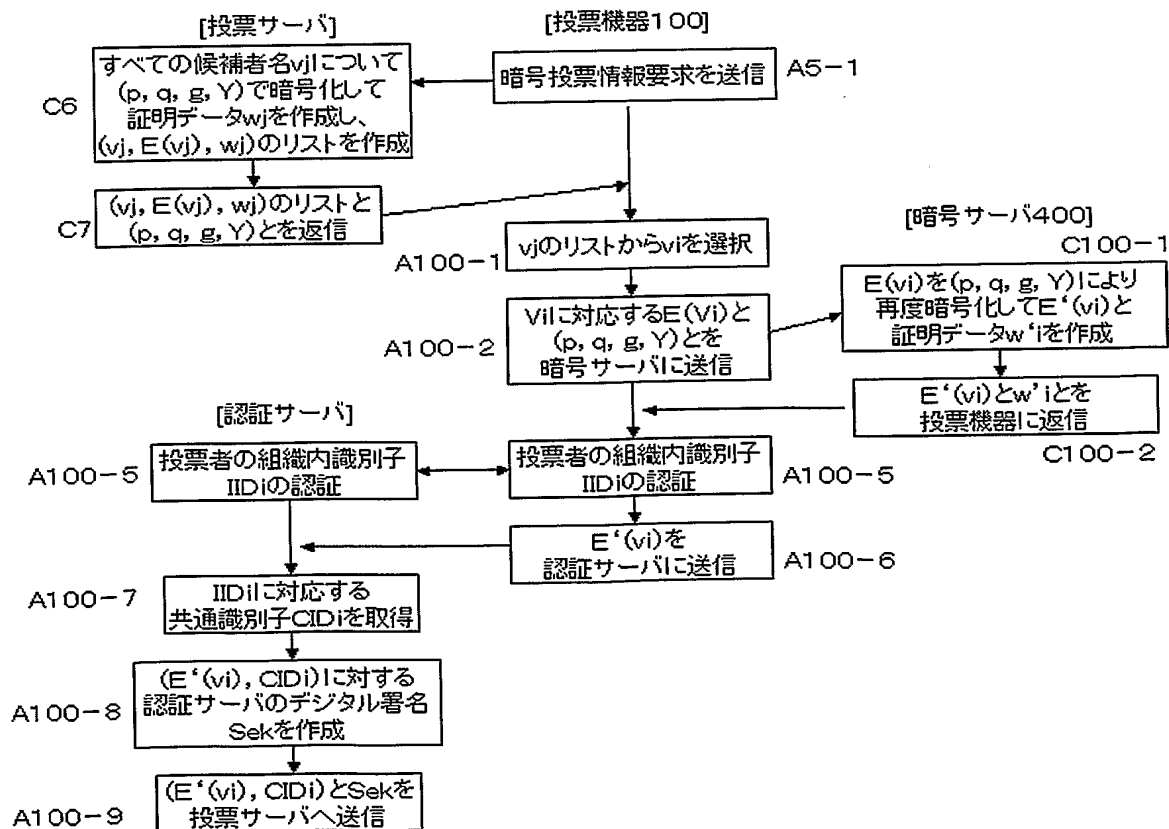
【図 14】



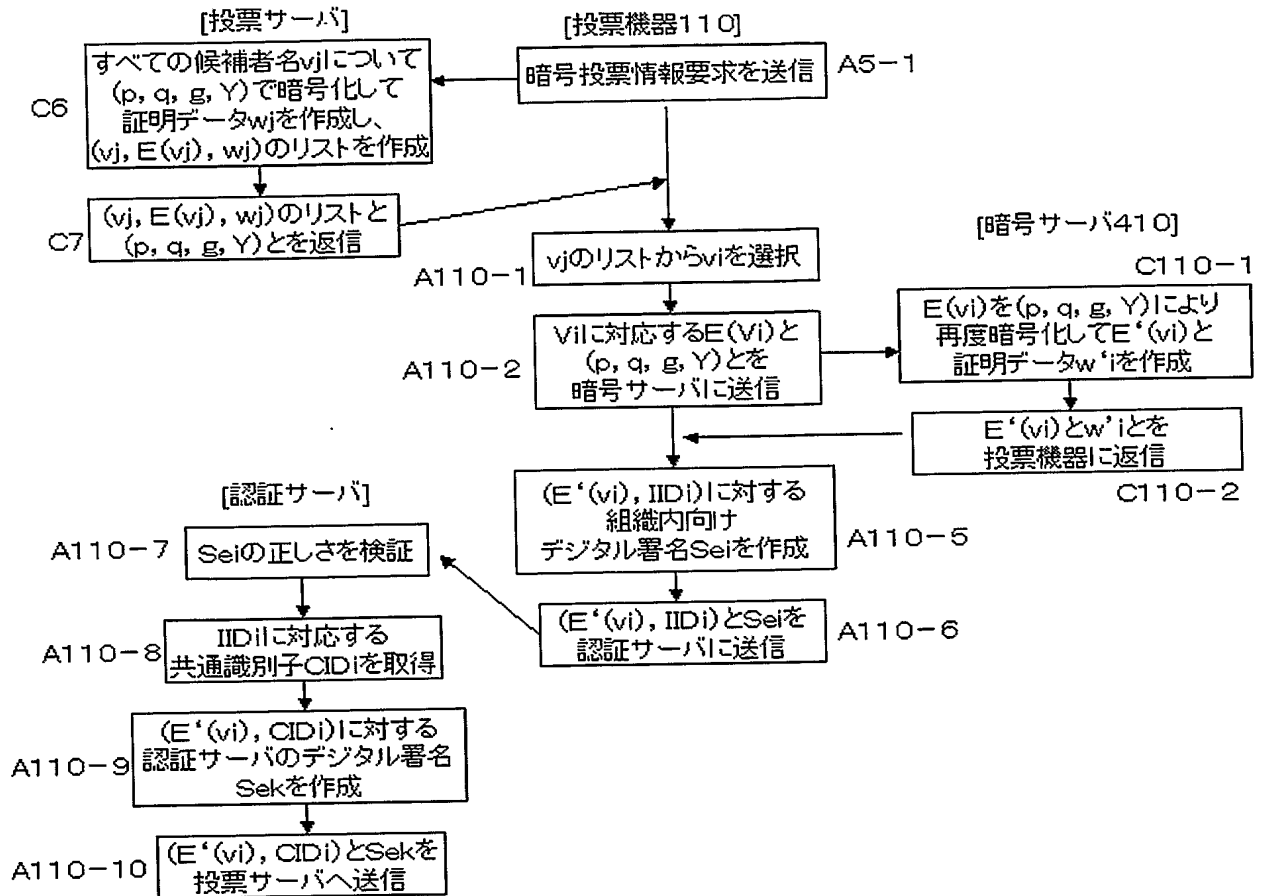
【図15】



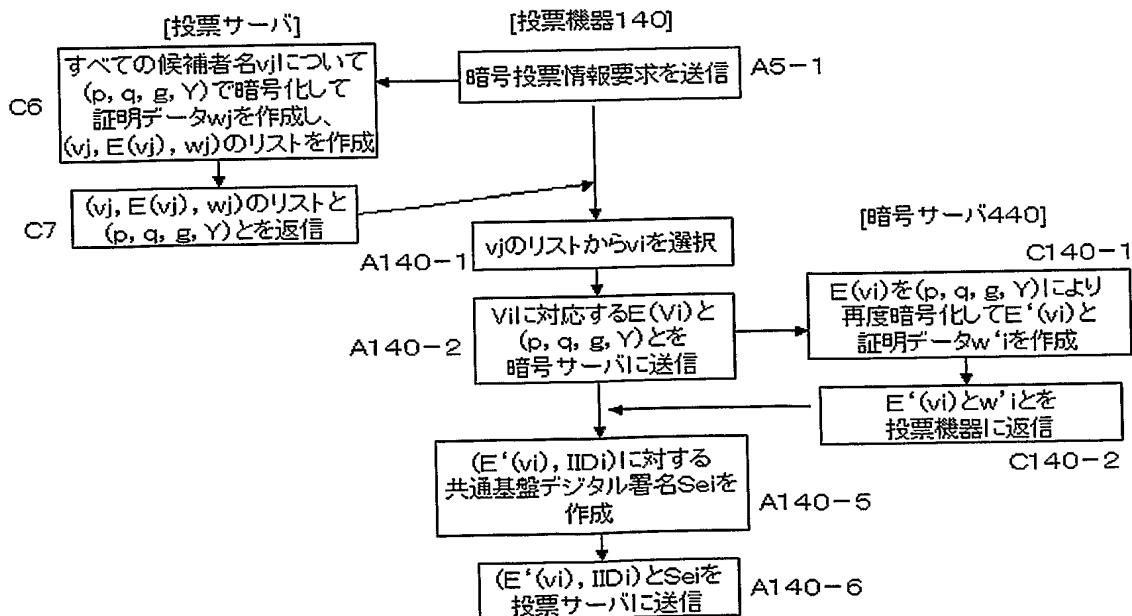
【図16】



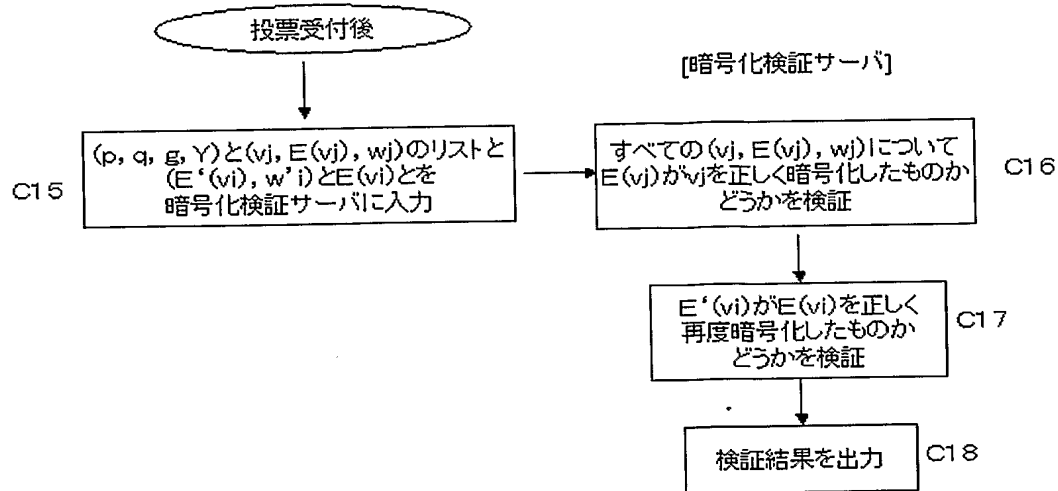
【図 17】



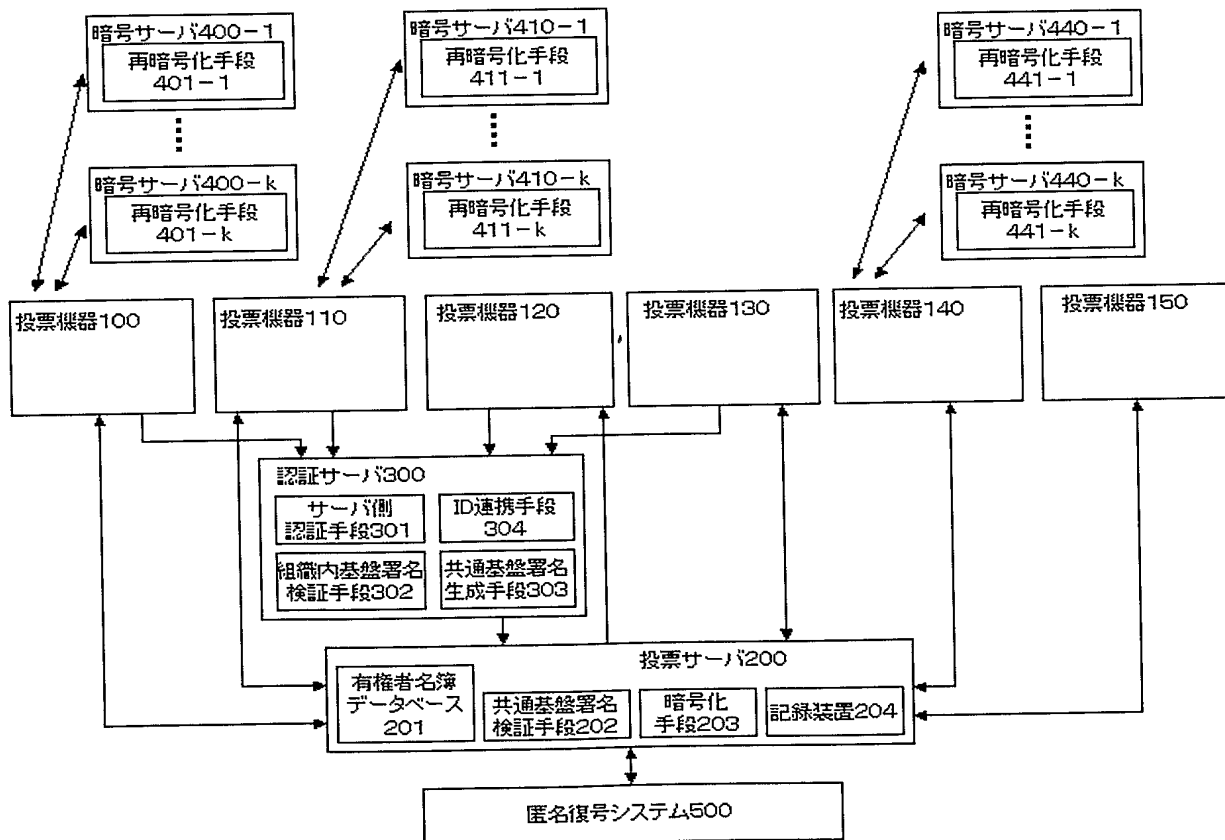
【図 18】



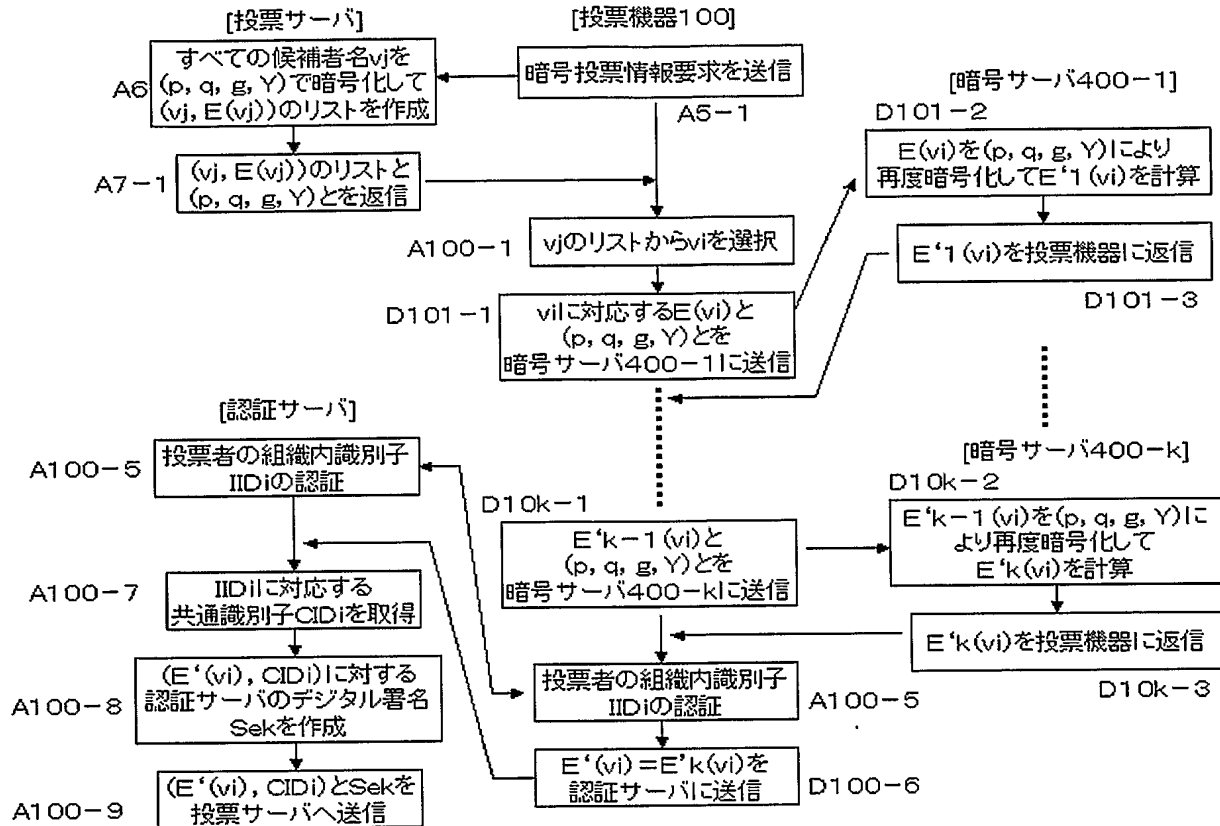
【図 19】



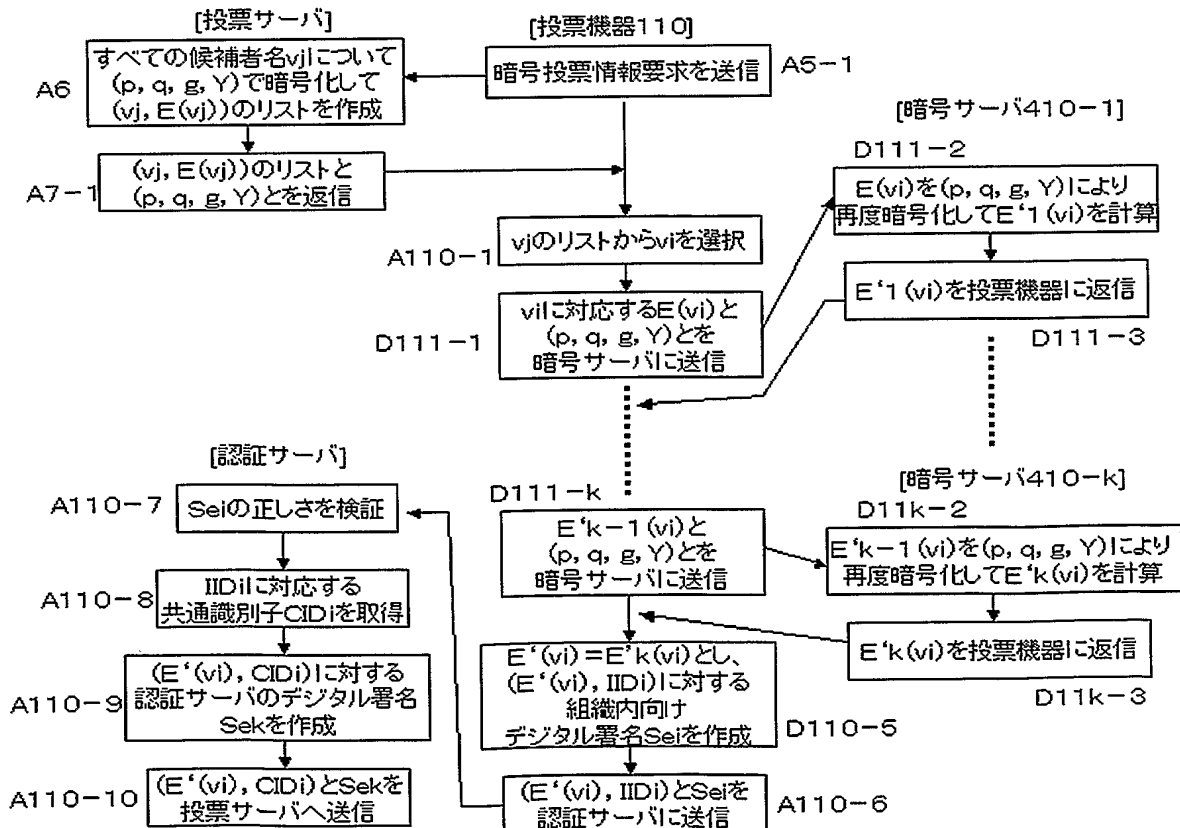
【図 20】



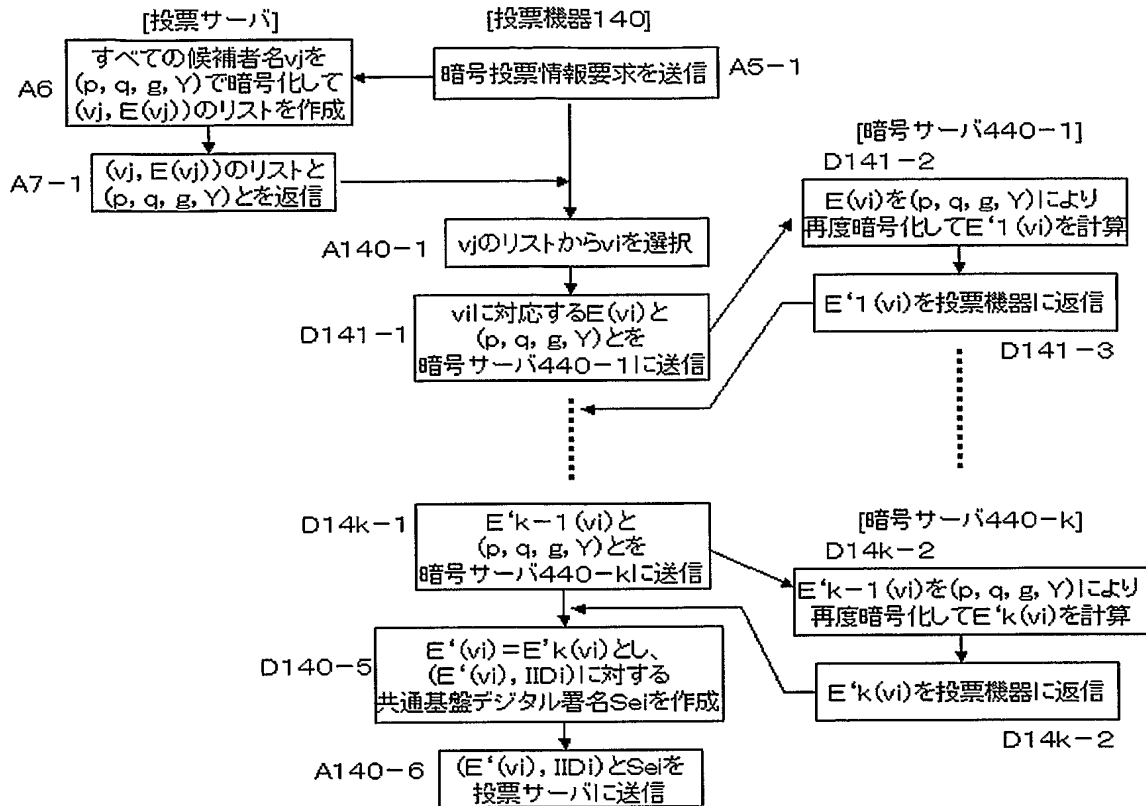
【図21】



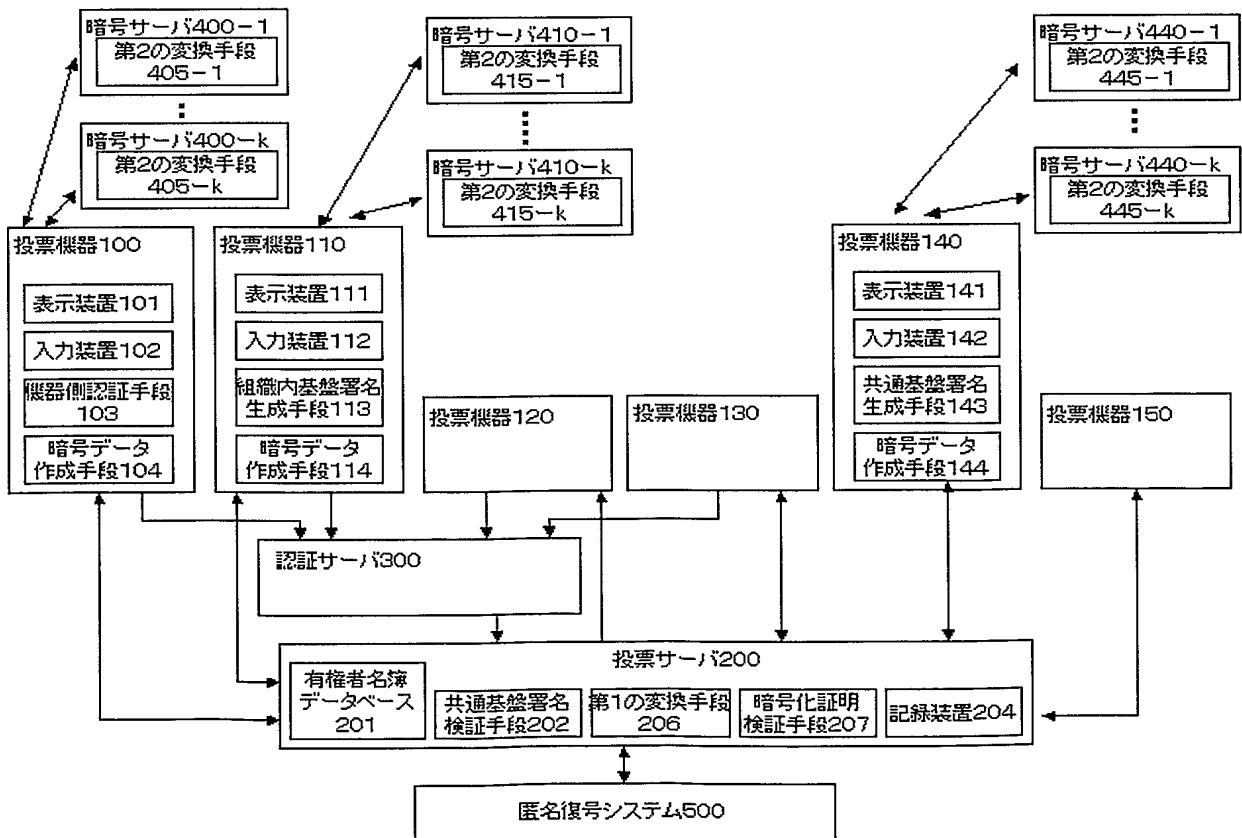
【図22】



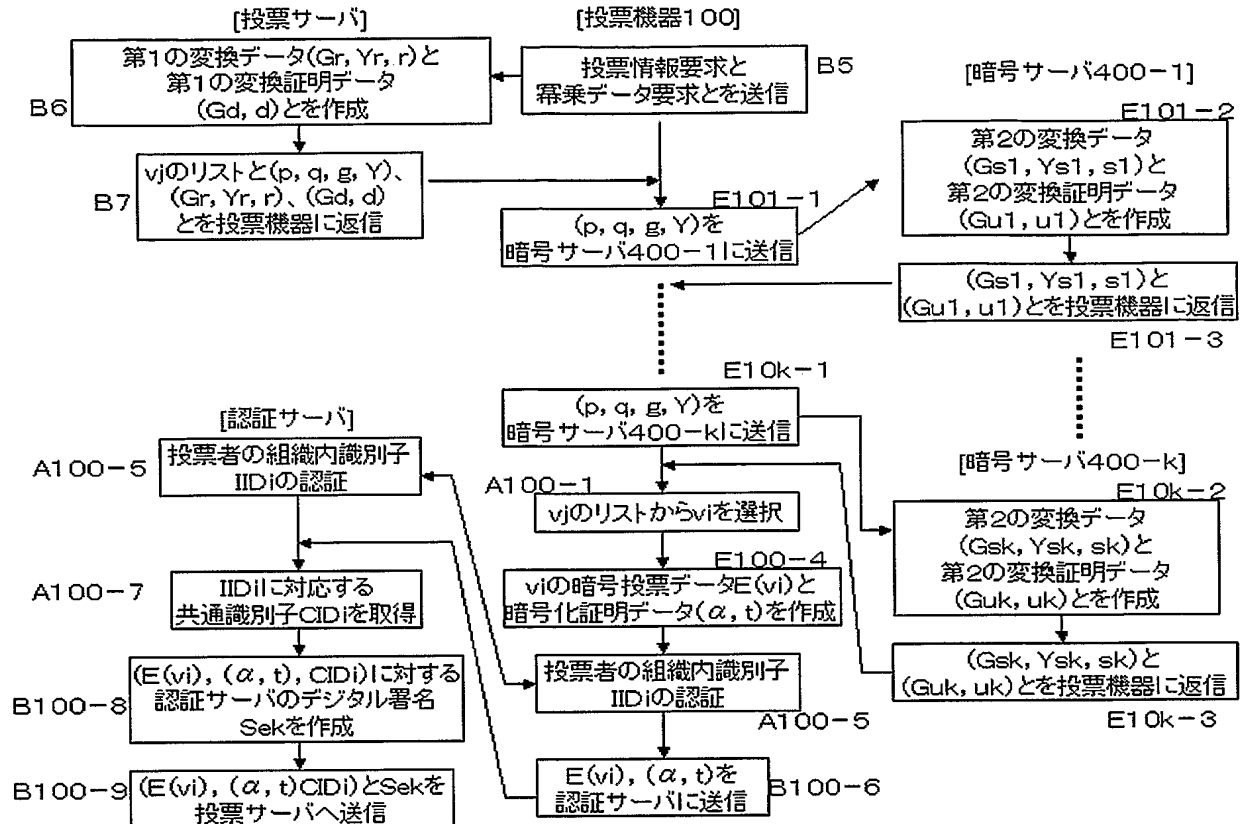
【図 2 3】



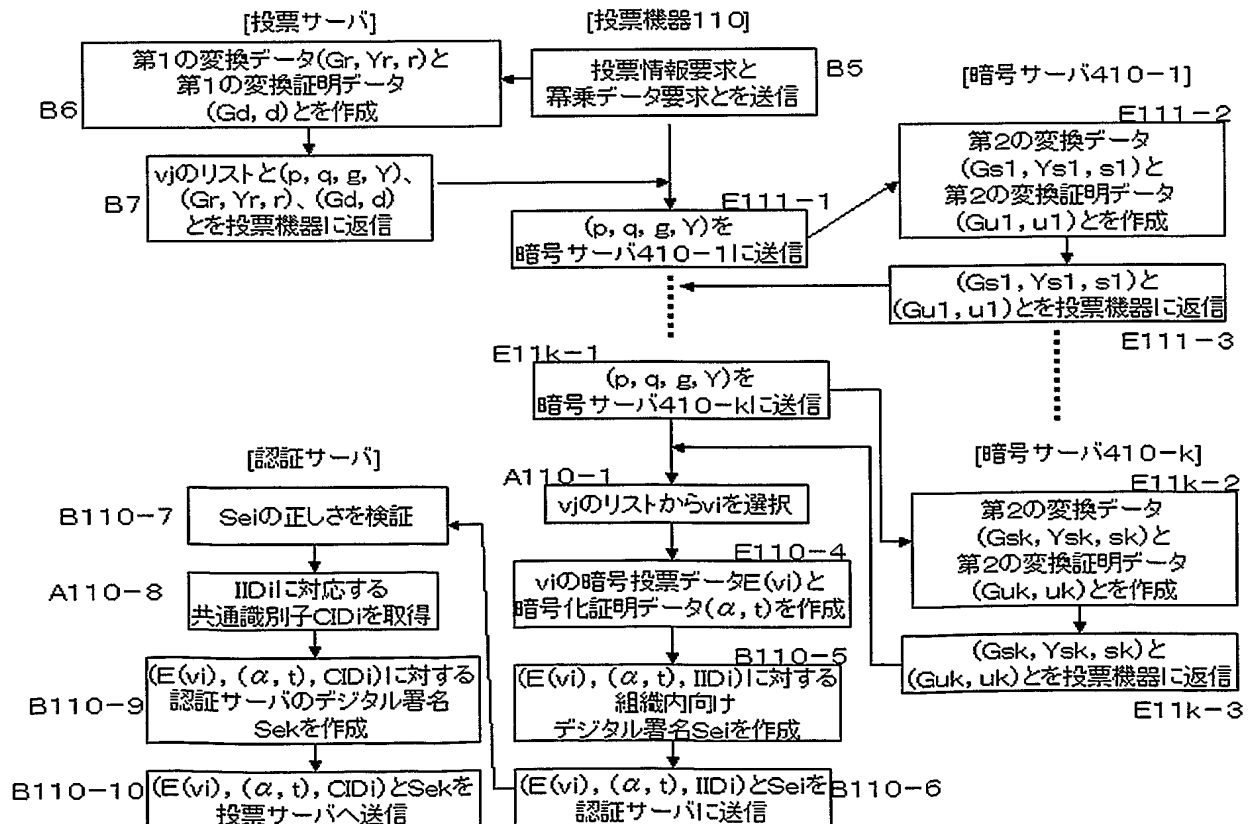
【図 2 4】



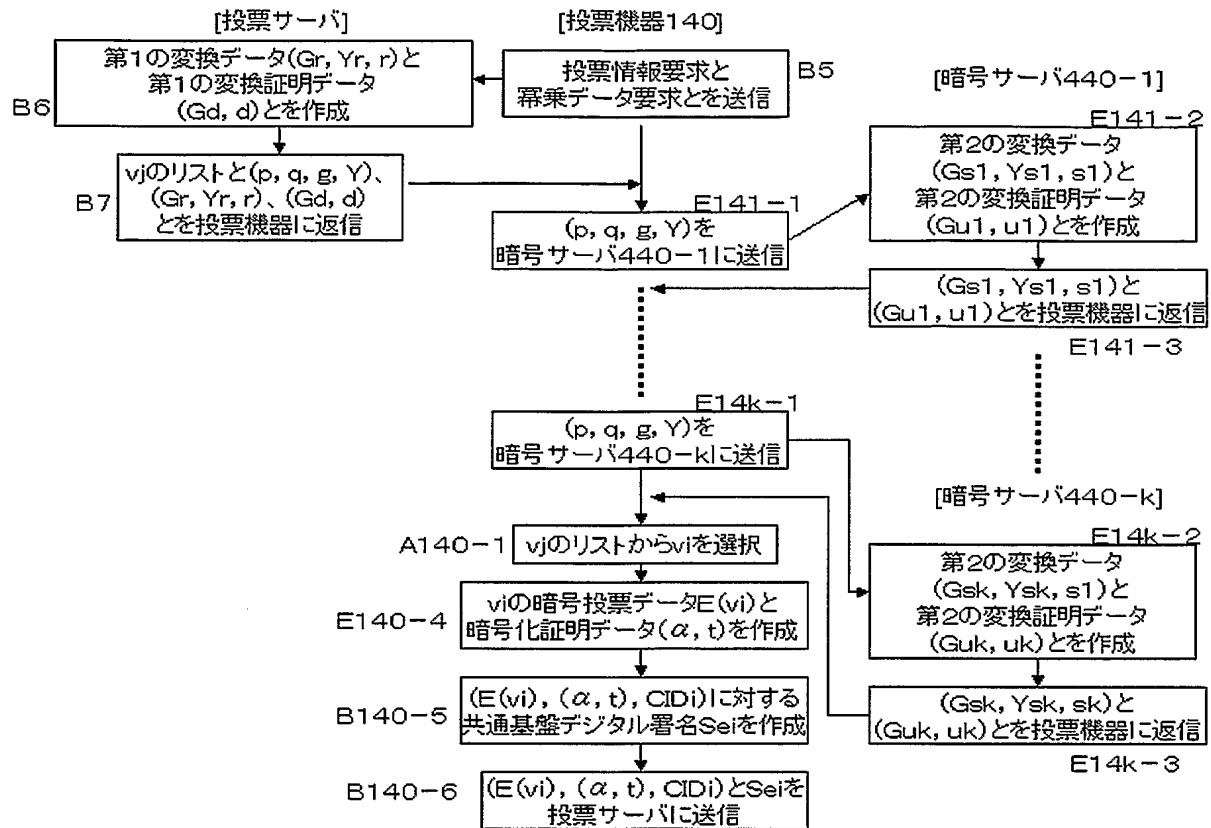
【図 25】



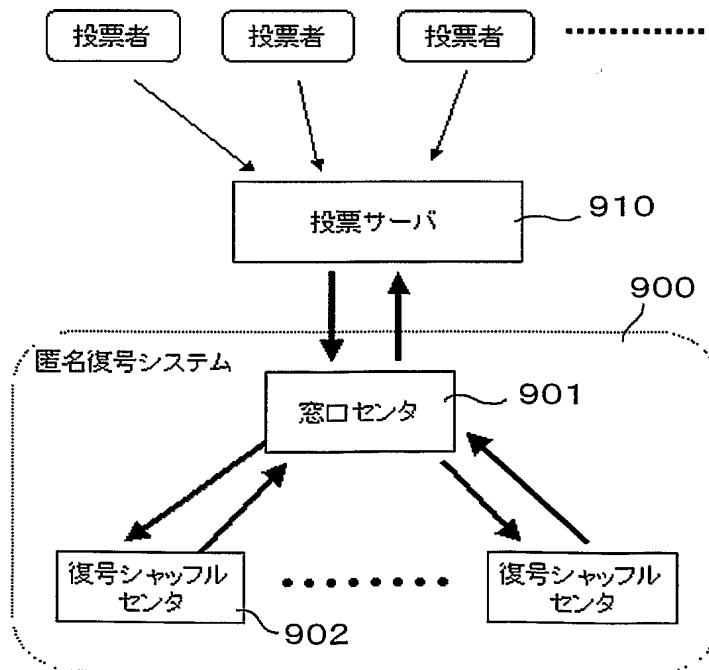
【図 26】



【図 27】



【図 28】



## 【書類名】 要約書

## 【要約】

【課題】 携帯電話などの記憶容量や処理能力の低い機器からの投票でも投票の秘密が守られ、また、全有権者に共通の公開鍵認証基盤が存在しない場合でも有権者認証を行えるようにする。

【解決手段】 投票サーバ 2 0 0 は、平文と平文を暗号化した暗号投票データとの組のリストを投票機器 1 0 0, …に送信し、投票機器 1 0 0, …は投票者の選んだ平文に対応する暗号投票データを暗号サーバ 4 0 0, …に送信し、暗号サーバ 4 0 0, …は暗号投票データを再度暗号化した暗号投票データを投票機器 1 0 0, …に返信し、投票機器 1 0 0, …は暗号サーバ 4 0 0, …から受信した暗号投票データを投票し、暗号投票データの復号には匿名復号システム 5 0 0 を用いる。投票機器 1 0 0, …は認証サーバ 3 0 0 に対して投票者の認証を行ない、また、暗号投票データに認証サーバ 3 0 0 が共通の公開鍵認証基盤によるデジタル署名を付与して投票サーバ 2 0 0 に送信する。

【選択図】 図 1

特願 2 0 0 4 - 0 1 6 8 9 4

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 4 2 3 7 ]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社